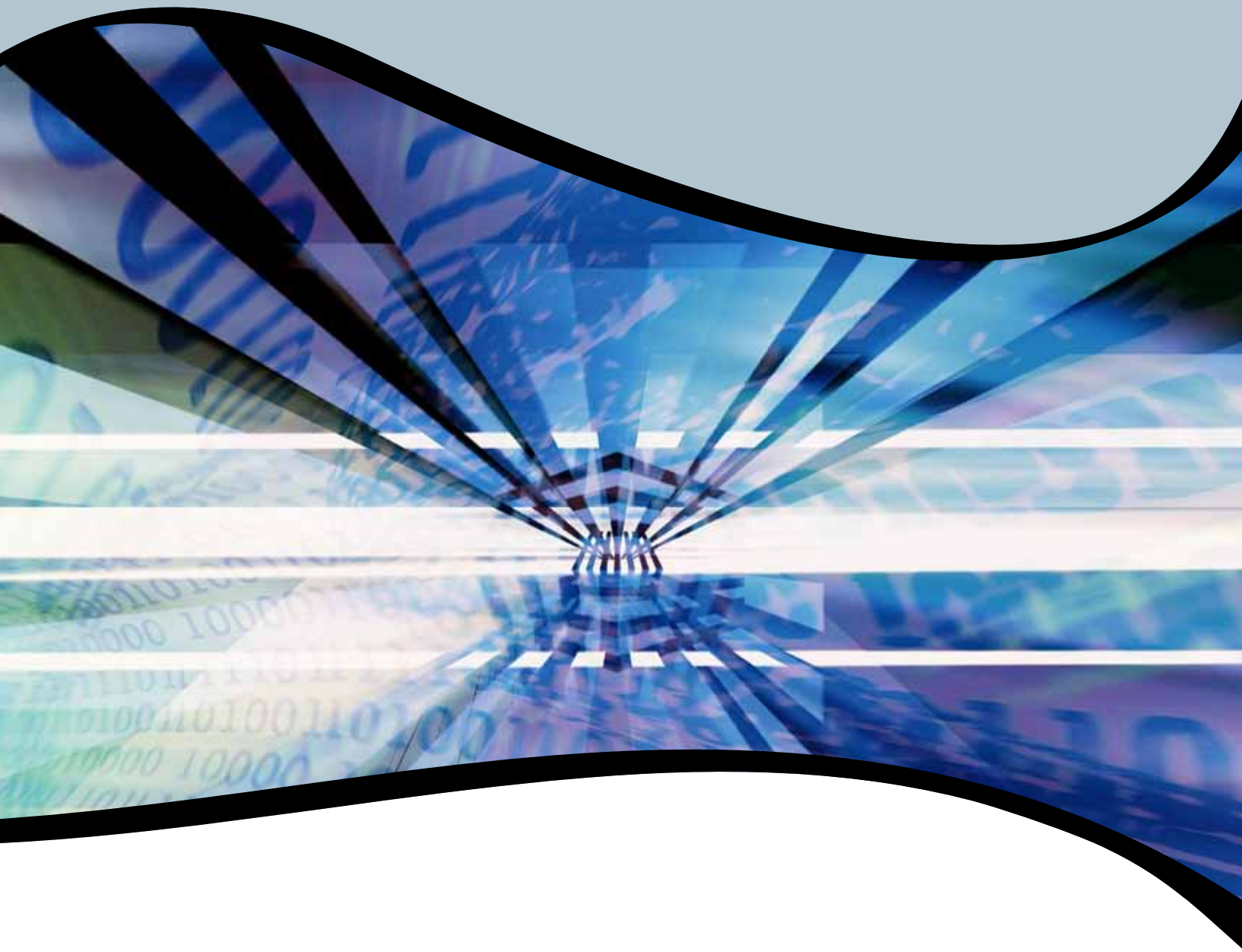
Tools

Information Assurance Tools Report

Sixth Edition

October 9, 2009

Firewalls



IATAC

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
09-10-2009	Report	09-10-2009

4. TITLE AND SUBTITLE

Information Assurance Technology Analysis Center (IATAC)

Tools Report – Firewalls. Sixth Edition

5a. CONTRACT NUMBER
SPO700-98-D-4002

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Revision by Holly Lynne M. Schmidt

5d. PROJECT NUMBER

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
13200 Woodland Park Road
Herndon, VA 20171

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
IATAC is operated by Booz Allen Hamilton, 8283 Greensboro Drive, McLean, VA 22102

14. ABSTRACT
This Information Assurance Technology Analysis Center (IATAC) report provides an index of firewall tools. It summarizes pertinent information, providing users a brief description of available firewall tools and contact information for each. IATAC does not endorse, recommend, or evaluate the effectiveness of any specific tool. The written descriptions are based solely on vendors' claims and are intended only to highlight the capabilities and features of each firewall product. The report does identify sources of product evaluations when available.

15. SUBJECT TERMS
IATAC Collection, Firewall

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Tyler, Gene
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	None	94	**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			703-984-0775

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Table of Contents

SECTION 1 ▸ **Introduction**

The Information Assurance Technology Analysis Center (IATAC) provides the Department of Defense (DoD) with emerging scientific and technical information to support Information Assurance (IA) and defensive information operations. IATAC is one of 10 Information Analysis Centers (IAC) sponsored by DoD and managed by the Defense Technical Information Center (DTIC). IACs are formal organizations chartered by DoD to facilitate the use of existing scientific and technical information. Scientists, engineers, and information specialists staff each IAC. IACs establish and maintain comprehensive knowledge bases that include historical, technical, scientific, and other data and information, which are collected worldwide. Information collections span a wide range of unclassified, limited-distribution, and classified information appropriate to the requirements of sponsoring technical communities. IACs also collect, maintain, and develop analytical tools and techniques, including databases, models, and simulations.

IATAC's mission is to provide DoD with a central point of access for information on emerging technologies in IA and cyber security. These include technologies, tools, and associated techniques for detection of, protection against, reaction to, and recovery from information warfare and cyber attacks that target information, information-based processes, information systems, and information technology. Specific areas of study include IA and cyber security threats and vulnerabilities, scientific and technological research and development, and technologies, standards, methods, and tools through which IA and cyber security objectives are being or may be accomplished.

As an IAC, IATAC's basic services include collecting, analyzing, and disseminating IA scientific and technical information; responding to user inquiries; database operations; current awareness activities (*e.g.,* the *IAnewsletter, IA Digest*, IA/IO Events Scheduler, and *IA Research Update*); and publishing State-of-the-Art Reports, Critical Review and Technology Assessments reports, and Tools Reports.

The IA Tools Database is one of the knowledge bases maintained by IATAC. This knowledge base contains information on a wide range of intrusion detection, vulnerability analysis, firewall applications, and anti-malware tools. Information for the IA Tools Database is obtained *via* open-source methods, including direct interface with various agencies, organizations, and vendors. Periodically, IATAC publishes a Tools Report to summarize and elucidate a particular subset of the tools information in the IATAC IA Tools Database that addresses a specific IA or cyber security challenge. To ensure applicability to Warfighter and Research and Development Community (Program Executive Officer/Program Manager) needs, the topic areas for Tools Reports are solicited from the DoD IA community or based on IATAC's careful ongoing observation and analysis of the IA and cyber security tools and technologies about which that community expresses a high level of interest.

Inquiries about IATAC capabilities, products, and services may be addressed to:

Gene Tyler, Director
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171
Phone: 703/984-0775
Fax: 703/984-0773

Email: *iatac@dtic.mil*
URL: *http://iac.dtic.mil/iatac*
SIPRNET: *https://iatac.dtic.mil*

1.1 Purpose

This report provides an index of firewall tools, which are also described in the IATAC Firewalls Tools Database. Firewall tools are constantly being added to the inventory to counter new threats. The tools listed in this Report are reviewed as of 5 June 2009. For this report, a firewall is defined as a component or set of components that restricts access between a protected network and an unprotected network (*e.g.,* the Internet) or other sets of networks while, at the same time, it facilitates authorized access to protected network resources through proxies, filters, and other mechanisms.

This report summarizes pertinent information, providing users a brief description of available firewall tools and contact information for each. IATAC does not endorse, recommend, or evaluate the effectiveness of any specific tool. The written descriptions are based solely on vendors' claims and are intended only to highlight the capabilities and features of each firewall product. These descriptions do not reflect IATAC's opinion. It is up to readers of this document to assess which product, if any, might best meet their security needs; however, the report does identify sources of product evaluations when available.

1.2 Report Organization

This report is organized into six distinct sections. Section 1 provides a brief introduction to IATAC and the Firewall Tools Report itself. Section 2 is a general overview of firewalls—what they are, why they are used, how they work, and the network models with which they work. Section 3 describes some of the various firewall technologies, including packet filtering, circuit-level gateway, application-level gateway, and stateful multilevel inspection. Section 4 reviews some of the major firewall considerations, such as the creation of an overall security policy and a specific firewall policy, how the firewall is to be managed, and product selection. Section 5 is a list of various firewall references. The final section of this report is a listing of currently available firewall products.

As a living document, this report will be updated periodically in hard copy, as well as our Web site *http://iac.dtic.mil/iatac.* Technical inquiries concerning this report may be addressed to IATAC at 703/984-0775 or *via* email to *iatac@dtic.mil*.

SECTION 2 ▸ Firewall Overview

2.1 What is a Firewall?

A firewall is a system of either hardware devices or software applications or a combination of both. The basic principle of a firewall is to block and permit traffic based on a security access control policy. The firewall system receives, processes, manages, and transmits information sent between two computer network enclaves. Traditionally, these enclaves are considered to be private networks plus the Internet. Typically, a firewall is installed at each access point on the perimeter of the private network, but security-oriented organizations frequently have firewalls established between segments of the internal private network or between the internal network and a permanent connection to partner network enclaves as well.

A hardware firewall is a device that sits between an internal private network and the public Internet. (See Figure 1.) Generally, this firewall permits you to connect multiple computers to it so that the computers may share a single Internet connection. These firewalls provide protection to all computers connected to it by using an Internet standard called Network Address Translation (NAT). NAT enables a network to use one set of internal private Internet protocol (IP) addresses that are translated to the firewall's public IP address. As a result, when an internal protected machine requests Internet information, the appliance firewall will convert the internal IP address to its public IP address, thus hiding the internal, private IP address. In turn, a network's hardware firewall accepts incoming data packets and forwards them to the requesting internal computer. This process ensures that outside machines do not directly connect to an internal computer.

A software firewall is an application that is installed on individual computers. (See Figure 2.) The software filters both inbound and outbound traffic and permits only the data that has been requested or explicitly permitted by a policy to pass through. Some organizations choose to use a combination of both hardware and software firewalls, assuming the added layer of security is worth the additional cost.

The decision regarding which type of firewall to use primarily depends on the needs of the user. Most organizations that have multiple computers connecting to the Internet opt for the hardware

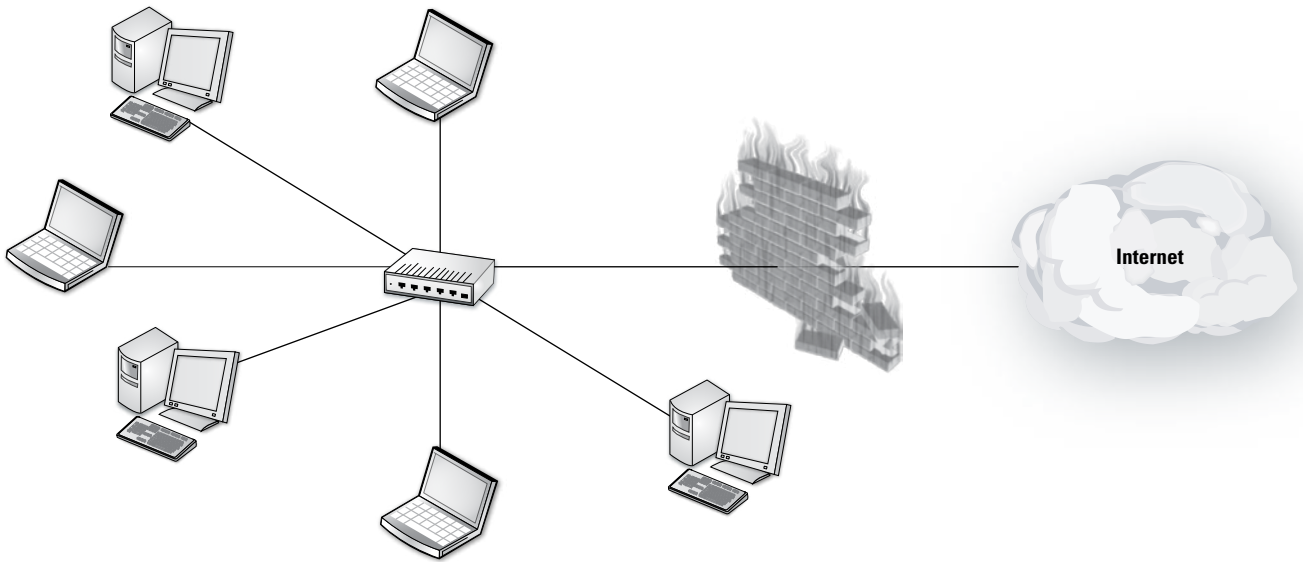


Figure 1 Hardware (Appliance) Firewall

firewall. Most home users do not require the robust capabilities of a hardware firewall and find the software firewall completely sufficient. Again, many will opt to use a blend of both hardware and software products. This combination not only adds a layer of security, but the personal firewall also provides greater functionality.

2.2 How Does a Firewall Work?

As mentioned earlier, the primary purpose of a firewall is to keep the bad guys out while still permitting the good guys get their job(s) done. This function is accomplished using access control, specifically through access and denial methodologies. After a packet is sent and screened by the firewall, the firewall may then permit the traffic through unless it meets certain criteria (rules), or it may deny the traffic unless it meets certain criteria. (See Figure 3.) The determining criteria for access or denial vary from one type of firewall to another. Firewalls permit or deny passage based on the type of traffic or on the source or destination addresses and ports. Rule bases that analyze the application data may also be used to determine if the traffic should be permitted. How this determination is made depends on which network layer the firewall operates.

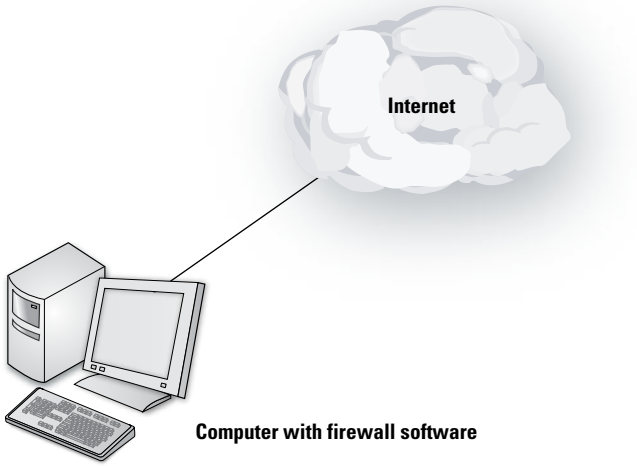


Figure 2 Software (Personal) Firewall

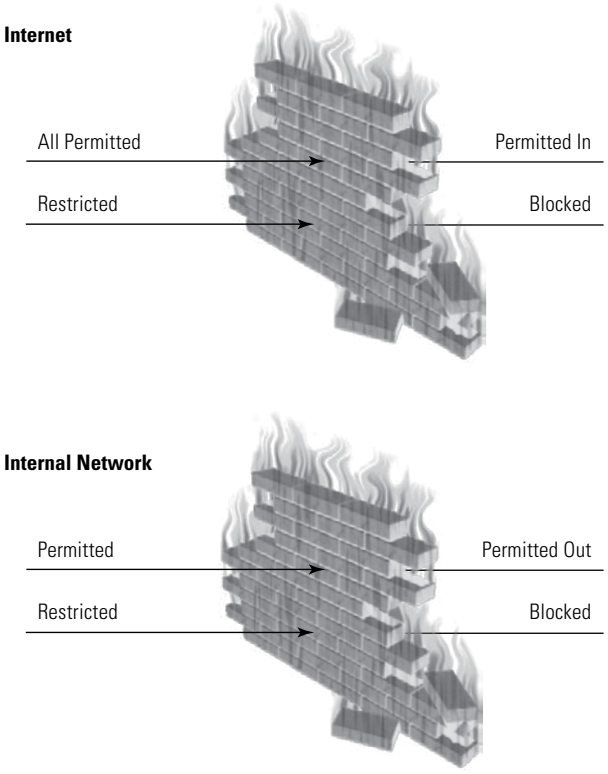


Figure 3 Basic Firewall Function

2.3 Network Models

To understand how firewalls really work, it helps to understand how the different layers of a network interact.

2.3.1 Open Systems Interconnection (OSI) Seven-Layer Model

Computers communicate and exchange data and information through a series of languages that are all governed by protocols. These protocols are the guidelines of how that data is formatted and packaged so that the destination computer, regardless of operating system or hardware platform, can process the data as intended. As computer network research and development progressed during the 1970s, the field grew so complex that the networking community recognized a need to establish a standard for networking communication. As a result, the International Standards Organization (ISO) created the Open Systems Interconnection (OSI) Seven-Layer model to permit countries and organizations around the world to communicate *via* computer protocols developed to this standard. The seven layers are

depicted in a stack formation with each layer of the stack responsible for a specific function. Another design aspect of the model is that the layers operate independently of one another and any layer can be redesigned, upgraded, or replaced without affecting the operation of the layers above and below the changed layer. The OSI Seven-Layer Model is as follows—

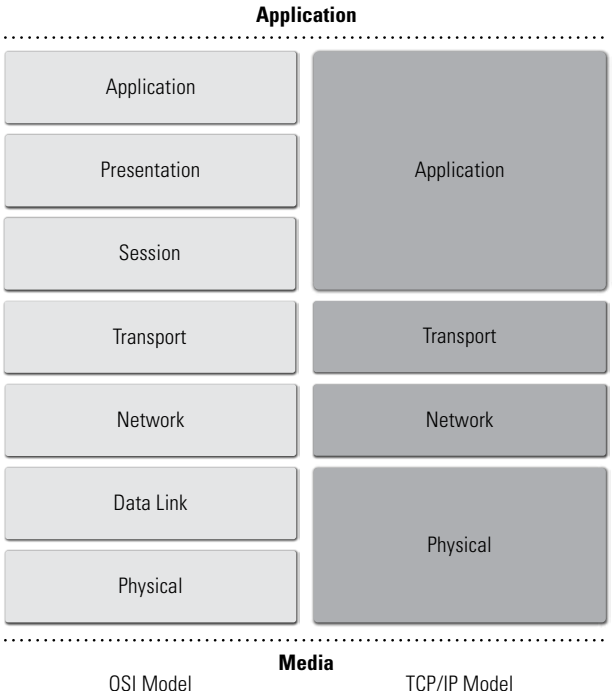


Figure 4 OSI and Transmission Control Protocol/Internet Protocol (TCP/IP) models

In this model, communication is initiated as a specific layer and sent to the layer below it, which in turn adds information specific to that layer and sends the new packet to the layer below it. The process continues until the packet reaches the physical layer and is sent over the network to the destination. Figure 4 shows this process of packaging or encapsulating data.

The receiving computer simply reverses the process—each packet destined for the receiving computer is copied from the network cable and passed to the layer above. Each layer processes the information specific to that layer and sends the packet to the layer above it, if necessary, until it reaches the appropriate layer and the payload of the packet is processed. Communication does not necessarily start and end at the application layer—it frequently happens at the lower layers, but is typically transparent to the end user. Firewall technologies operate at various layers because determined adversaries will always employ exploitation methods and techniques at as many layers as necessary to accomplish their goal.

As firewall products have evolved, they have been designed to operate at different layers within the OSI model. Firewalls that operate at the lower (numerical) layers in the OSI model tend to be less sophisticated and are therefore less complicated to establish and maintain. These types of firewalls tend be transparent to the network user and perform well with higher throughput volumes. Because of lower overhead, these devices typically do not examine the actual data being transmitted within each packet, and because these types of firewalls operate at lower layers in the OSI model, knowledgeable adversaries can readily circumvent the security they provide. These firewalls are still useful and a valuable part of a network security architecture, as we will discuss in Section 3 of this report. Firewall devices that operate at higher (numerical) layers in the OSI model, such as a proxy server, tend to be more complicated devices that evaluate the validity of the data content within each transmitted packet and even maintain internal information about the state of connections passing through the firewall. This sophistication and thoroughness come at the price of processing-power requirements.

2.3.2 Transmission Control Protocol/ Internet Protocol (TCP/IP) Stack

While the OSI Seven-Layer model presents a framework or standard for network communication, the most prevalent network communication protocol suite in use today is the Transmission Control Protocol/Internet Protocol (TCP/IP). There are many variations of the TCP/IP protocol stack, but the most widely adopted version is the DoD model, which is depicted as only four layers instead of the OSI model's seven layers. (See Figure 4.)

2.3.2.1 Application Layer

The top layer in the Internet reference model is the Application Layer. This layer provides interface support for users or their programs, provides such functions as encryption and compression, and is responsible for communication session start-up and tear down. Services such as file transfer protocol *(FTP)* and hypertext transfer protocol *(HTTP)* operate at the Application Layer. The Application Layer in DoD's TCP/IP model is effectively equivalent to the Application Layer, the Presentation Layer, and the Session Layer in the OSI Seven-Layer Model. One difference in nomenclature between the two models is that the OSI model refers to communication between two computers as a session, while the TCP/IP model refers to the start and destination points—the IP address and the port number are combined to create a socket.

2.3.2.2 Transport Layer

The protocol layer just below the application layer is the Transport Layer. The Transport Layer is responsible for providing end-to-end data integrity. As the name implies, the Transmission Control Protocol (TCP) operates at the Transport Layer. TCP is connection-oriented and provides delivery verification and guarantee for data transmitted across the network. This is analogous to a telephone call—a connection is made, the data is transferred in sequential order, the receiving party can provide immediate feedback if the data was interrupted so that the data can be retransmitted, and then the connection is terminated. Another transmission protocol that operates at the Transport Layer is the user datagram protocol (UDP), which does not guarantee datagram delivery. Instead, delivery verification is left to the Application Layer. This would be analogous to sending a phone book, one page at a time, through standard postal mail. The sender does not know if the recipient receives all pages or in what order—that is the responsibility of the recipient. The Transport Layer in the DoD's TCP/IP model performs the same functions as the Transport Layer in the OSI Seven-Layer Model.

2.3.2.3 Network Layer

The layer below the Transport Layer is called the Network Layer. This layer is responsible for routing messages between networks. This is the layer that most router devices operate, as does the IP protocol of the TCP/IP stack. The Internetwork Layer in the DoD's TCP/IP model performs the same functions as the Networking Layer in the OSI Seven-Layer Model.

2.3.2.4 Physical Layer

The Physical Layer is the lowest layer in the DoD's TCP/IP reference model. This layer is responsible for transmitting and receiving the frames of data across the network to and from the network's physical wiring and cables. The Network Interface Layer is also responsible for correctly implementing the address scheme and for modifying frames that are destined for the local network segment by changing the addressing scheme to the destination computer's media access control (MAC) address. The MAC address is physically burned into every network interface card (NIC) and uniquely identifies it on the network. The protocol that is used at the Network Interface Layer to accomplish this is the address resolution protocol (ARP). The Network Interface Layer performs the same functions as the Data-Link Layer and Physical Layer in the OSI Seven-Layer Model.

2.4 Why Use a Firewall?

Firewalls help safeguard your computer and other network resources by enforcing restrictions on network traffic while still permitting user access to the public network. They can also help mask your computer's identity, so hackers' attempts to probe or scan your computer will not provide any useful information.

The layering of IA solutions within information technology (IT) assets is known as defense-in-depth (DiD), and you can add an important layer of protection to your network by installing a firewall. Potential intruders may scan computers on the Internet, probing for an opening they can use to gain access. A firewall can help block unauthorized entry into your computer and restrict outbound traffic.

While IA is not accomplished solely by installing a firewall on the perimeter of a network system, it is one aspect of a well-planned computer network security posture and is an important component of creating an environment that is both secure and functional.

2.4.1 What a Firewall Can Do

A firewall examines all traffic routed between two networks to see if it meets certain criteria. When a firewall receives a packet from either a trusted or an untrusted source, it must determine whether or not that packet should be forwarded on to the computer network enclave, modified before forwarding, or stopped altogether. The firewall can process the packet in several different ways, depending on the type of firewall technology it uses. In most cases, a firewall will use a pre-configured list of parameters and thresholds to permit or deny the packet transmission. The following list presents and describes some of the more common firewall features and capabilities—

- **Block, filter, or permit/allow traffic, based on source or destination address**—Firewalls can permit or deny any type of network traffic, regardless of its content, based on its source or destination address. This is a common practice for corporate perimeter firewalls and is intended to prevent not only nefarious individuals attempting to gain unauthorized access to the corporate network but also to prevent employees from visiting nonproductive Web sites or Web sites that contain material violating corporate policies.
- **Block, filter, or permit/allow traffic, based on content within the traffic**— Firewalls can completely permit or deny or simply filter network traffic based on the data within the traffic. A common scenario of this operation is email with virus-infected attachments—the firewall can either deny the email traffic entirely, or it can remove the attached file and still forward the email message to the other side of the firewall.
- **Extend the internal network to include remote users**—Some firewalls can be used to provide secure connections to remote users and to include those users as part of the trusted network. This is accomplished using virtual private network (VPN) products that are being incorporated into firewall products for a seamless integration.
- **Log and report all denied traffic**—Firewalls can log data to determine the health status of the firewall itself and determine anomalous behavior (potential security violations) through subsequent analysis of the data. The logged data can also be used to create reports based on traffic trends and patterns. Logged data can prove to be invaluable when network administrators are trying to determine how and when an intruder gained access to internal network resources.
- **Establish and hide network clients**— Some firewalls can be configured to provide network address information to clients in a trusted enclave *via* the dynamic host configuration protocol (DHCP). Firewalls can also effectively hide the trusted enclave from the untrusted enclave if the addressing scheme of the trusted enclave is private or non-routable, over the Internet (*e.g.,* internal addressing schemes 10.x.x.x, 172.16-31.x.x, and 192.168.x.x). The firewall can hide these clients by NAT, which associates the client's non-routable address with a valid routable address on the untrusted enclave. This process is automatically performed by the firewall and is completely transparent to the client.

2.4.2 What a Firewall Cannot Do

A firewall has specific security capabilities and limitations. As previously stated, it is only one aspect of DiD. There are several common misconceptions about what a firewall can and cannot do. Below is a listing of a few things that firewalls cannot perform.

- **Prevent attacks that are not trafficked through the firewall**—This may sound painfully obvious, but a firewall cannot block and/or filter network traffic that does not pass through the firewall. This is an important reminder that "the chain of security is only as strong as the weakest link," and that every access and egress point from a network must be monitored and secured. If the network has multiple external connections that are not secured

by firewalls, adding a firewall at the main connection to a network does not provide comprehensive security.

- **Prevent malicious code**—Firewalls cannot prevent malicious code from spreading throughout a trusted environment when an employee introduces viruses to the network. If an employee installs infected, unauthorized software or connects an infected laptop to an internal network, a firewall offers no protection to other hosts on the internal network. For additional details related to this topic, consult the IATAC Tools Report on Anti-Malware.
- **Prevent espionage or data theft**— Firewalls cannot prevent espionage or data theft if a corporate network is connected in multiple places to other networks (such as the Internet) without a firewall in place at every external network connection.
- **Prevent distribution of corporate trade secrets**—Firewalls cannot prevent theft and distribution of corporate trade secrets or intellectual property by disgruntled employees.
- **Prevent social engineering attacks**—Firewalls cannot prevent social engineering attacks that result in an unsuspecting network user having his/her user name and password information provided to an adversary posing as a support staff member.
- **Monitor suspicious network activities**—Monitoring suspicious activity is not the main function of a firewall. While firewall logs can be used to help determine suspicious activity, an intrusion detection system (IDS) can best perform this functionality. For additional information pertaining to IDS, consult IATAC's Intrusion Detection Systems Report.

SECTION 3 ▶ Firewall Types and Technologies

The most commonly known firewall technologies include the following—

- **Packet filtering**
- **Circuit-level gateways**
- **Application-level gateways**
- **Stateful multilevel inspection**

3.1 Packet Filtering

Packet filtering is the most rudimentary of the technologies and does just what its name implies—filter packets. A packet is basically a unit of data that is broken into three pieces—a header, the payload, and a trailer. It is the header of a packet that contains the information used for determining if the packet is permitted or denied. A packet is passed through the firewall, where the header information is then compared to a predetermined rule set. Based on this comparison, the packet is then forwarded or dropped. As an example, if a packet-filtering firewall were configured to block all data traveling out using port 80 (the standard port for *HTTP),* the effect would disable all computer Web browsing from inside the firewall. Packet-filtering firewalls are the most basic of the technologies in that they do not care about data content, only the data's destination. Circuit-level gateways are a bit more sophisticated in their functionality.

3.2 Circuit-Level Gateways

Similar to the packet-filtering firewalls, circuit-level gateways are also able to filter traffic by IP address and port, but they go a step further in that they validate the actual connection before any data is passed. What this means is that when a session is opened, traffic is only permitted from a specifically requested source and for a finite amount of time. When a source computer initiates a request for a session, the gateway reviews this request and passes it on to the destination server, making it appear as if the request is now coming from the gateway. This process is a form of NAT, which was addressed in Section 2.1. The server then sends the requested data back to the gateway, where the information is compared to the original request. If the IP address and port match, the information is permitted to pass. With this firewall technology, only requested information is permitted to pass through the firewall. Application-level gateways are very similar to circuit-level gateways but are a bit more in depth.

3.3 Application-Level Gateways

Application-level gateways, also known as proxies, are very similar to circuit-level gateways. How they handle the information is the big difference between the two. An application-level gateway takes the connection inspection to a new level by reviewing the application layer of a connection, thus providing a higher level of security. Proxies can inspect specific commands made by an application (*e.g.,* the GET command in *HTTP).* It can also inspect user activity such as log-ins and file access and apply different rules for different authenticated users. Very detailed logs about network activity can be generated from an application-level gateway; however, because of this level of detail and complexity, network performance can be significantly impacted. Also, the firewall must be configured for every type of application used on the network. If a new type of application is created, a module or upgrade must be added to the device.

3.4 Stateful Multilevel Inspection

Stateful multilevel inspection firewalls apply a combination of packet filtering, circuit-level gateway, and application-level gateway firewalls. These firewalls filter packets at the network layer, review session packets before permitting them to pass, and review information at the application level. They permit direct connection between client and host, thus alleviating issues caused by the lack of transparency in application-level gateways. Also, instead of using the same application-level filtering in other firewalls, these devices use algorithms that reduce the resources required to inspect packets at the application level. In addition, there are no application-specific proxies that must be installed every time a new application is used on the network. Stateful multilevel inspection devices create the highest level of security and also have good performance—but they are very expensive. The cost includes the resources to configure the device. The rule set for these devices is very complicated, and if it is not properly configured, the firewall may not be secure. The complex rules allow a more secure perimeter; however, configuration requires a skilled security team, or the rules will not be properly configured and may result in a less secure network.

3.5 Firewall as part of a Security Suite

Because installing a firewall is one of many network security techniques, firewall products are sometimes incorporated as part of a network security "suite," or tools package. Some of these packages include VPN, antivirus, intrusion detection, or other monitoring software. Firewalls that are part of a suite may be any of the types of firewalls listed previously, but because they are bundled with the suite purchase, have been categorized separately.

3.6 Personal Firewalls

Personal firewalls differ from the rest of the firewalls in this report based on their scale. Personal firewalls are intended for individual workstations or a relatively small network. This type of firewall may be a cheaper alternative to protect a small number of workstations, rather than using a large enterprise license or appliance. Additionally, this type of firewall can be used by employees who use personal computers to perform work. Like suite software, some personal firewalls package VPN, antivirus, spyware, or other monitoring software in a single application.

SECTION 4 ▶ Considerations

4.1 Security Policies

"Perfect security" is not a realistic objective for enterprise networks. As long as humans are involved, there will always be residual risk within networks of information systems. The most secure network environments—those that implement and vigilantly maintain security measures—may approach the ultimate goal of total security, but will never reach it because mistakes and improper configurations will ensure that every publicly available network will be vulnerable to attack however briefly. These mistakes and improper configurations include everything from operating system and application design flaws to improperly configured email filters and firewall rule sets. Therefore, the first step in providing security for a network environment must be to create a well-thought-out, consistently implemented security policy. In general, policies define what behavior is permitted and not permitted and help define which tools and procedures an organization requires. A firewall policy helps to enforce the overall security policy, establishes how a firewall should handle application traffic, and establishes how the firewall should be managed and updated.

4.2 Firewall Management

Large network enclaves, such as a corporate computer network environment, frequently have more than one access point to and from the enclave. For this reason, installing firewalls requires managing firewalls. To manage any firewall, all aspects of management and maintenance must be documented, staff roles and responsibilities must be outlined, and many other decisions must be considered, such as the following—

- What type of network traffic and data requests will be permitted to pass through the firewall?
- Will multiple firewalls be managed from a central location or on an individual basis?
- How many firewall administrators will have administrative access to each firewall?
- What is the process to request adding, modifying, and/or deleting rules from a firewall?
- Who is responsible for implementing changes to a firewall rule set?
- Who will maintain backup copies of the firewall rule sets and how will this be accomplished?
- Who is responsible for monitoring the health status of each firewall to ensure continued proper operation?
- What types of network traffic and events will be logged by each firewall?
- Who and how often will those firewall logs be reviewed for suspicious activities?
- How will suspicious network activities be addressed once they have been identified?

4.3 Firewall Product Selection

After determining that a firewall is required, there are still several considerations that should be thoroughly evaluated before selecting a firewall. These considerations include the following—

- Is there a network security policy that must be enforced by the firewall? What are the technical requirements of this policy?
- What are acceptable levels of risk associated with specific types of data and services that are being offered?
- What firewall features and technologies will be required to meet the above requirements and network services?
- What are the total costs to purchase, implement, support, maintain, and update or upgrade the firewall product?
- What type of monitoring, logging, and auditing will the firewall be required to provide?
- What is the scalability of the firewall product, or what other benefits and features does each firewall product offer that may support future growth of the organization or additional security requirements?
- If the firewall is to be managed internally by the organization's staff, does the staff have the appropriate technical skills?

SECTION 5 ▶ Firewall References

The following section provides additional references in the form of books, mailing lists, and web sites. This list is arranged by publication date, with the most recent publication date first.

5.1 Books

The Best Damn Firewall Book Period, Second Edition (PB)

Authors	Cherie Amon, Thomas W. Shinder, Anne Carasik-Henmi
Publisher	Syngress Publishing
Edition	November 2007
ISBN	1-59749-218-3

Firewall Fundamentals

Authors	Wes Noonan, Ido Dubrawsky
Publisher	Cisco Press
Edition	June 2006
ISBN	1-58705-221-0

CheckPoint NG VPN-1/Firewall-1: Advanced Configuration and Troubleshooting, 2nd Edition (PB)

Authors	Barry J. Stiefel, Doug Maxwell, Kyle X. Hourihan, Cherie Amon, James Noble
Publisher	Syngress
Edition	June 2003
ISBN	1- 93183-697-3

Firewalls and Internet Security: Repelling the Wily Hacker, 2nd Edition (PB)

Authors	William R Cheswick, Steven M. Bellovin, Aviel D Rubin
Publisher	Addison Wesley Professional
Edition	February 2003
ISBN	0-20163-466-X

Cisco Security Specialist's Guide to Private Internet Exchange (PIX) Firewalls (PB)

Authors	Umer Kahn, Vitaly Osipov, Mike Sweeney, Woody Weaver
Publisher	Syngress Publishing
Edition	December 2002
ISBN	1-93183-663-9

Firewall Architecture for the Enterprise (PB)

Authors	Norbert Pohlmann, Tim Crothers
Publisher	Wiley
Edition	July 2002
ISBN	0-76454-926-X

Building Internet Firewalls, 2nd Edition (PB)

Authors	Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman
Publisher	O'Reilly Media
Edition	January 2000
ISBN	1-56592-871-7

5.2 Mailing Lists

▶ CheckPoint Firewall-1 Mailing List
http://www.checkpoint.com/services/mailing.html

The CheckPoint Firewall-1 mailing list is a discussion forum for firewall administrators and implementers geared specifically to the FW-1 product line.

- Firewall-Wizards Mailing List
  https://honor.icsalabs.com/mailman/listinfo/firewall-wizards

The purpose of this list is to provide a moderated firewall and security-related list that is more like a journal than a public soapbox. Firewall-Wizards will not be cluttered with spam, flames, or other non-list-related traffic. The addresses of the list members will not be made available for any purpose other than maintaining the list. This is because participation on this list should not be an invitation to unnecessary junk mail.

- Firewall Product Developer's Consortium
  https://www.icsalabs.com/icsa/topic.php?tid=jgjgjg$dsf-sfddf

"The ICSA Labs Firewall Product Developer's Consortium (FWPD) was established in 1995 to provide a forum in which developers of competing firewall products could work toward common goals to benefit both members and end users. Since then, it has developed into an international group dedicated to collectively identifying and solving today's Internet security problems."

5.3 Web Sites

- International Computer Security Association (ICSA) Labs
  https://www.icsalabs.com/icsa/main.php?pid=gddfg

A commercial lab that evaluates the security of commercially available products—in this case, firewalls—based on specific testing criteria that are also detailed on their Web site.

- The Common Criteria Evaluation and Validation Scheme (CCEVS)
  http://www.niap-ccevs.org/cc-scheme/

The focus of the CCEVS is to establish a national program for evaluating IT products for conformance to the International Common Criteria for Information Technology Security Evaluation.

- Computer Security Resource Center
  http://csrc.nist.gov/publications/PubsSPs.html

This site is devoted to sharing information security tools and practices, providing one-stop shopping for information security standards and guidelines, and identifying and linking key security Web resources to support the industry.

- Home PC Firewall Guide
  http://www.firewallguide.com/

This Web site provides easy access to basic information about, and independent, third-party reviews of, Internet security and privacy products for home, telecommuter, and Small Office, Home Office (SOHO) end users.

SECTION 6 ▶ **Firewall Tools**

Section 6 summarizes pertinent information, providing users a brief description of available firewall tools and vendor contact information. Again, IATAC does not endorse, recommend, or evaluate the effectiveness of these tools. The written descriptions are drawn from vendors' information and are intended only to highlight the capabilities or features of each product. It is up to the reader to assess which product, if any, may best suit his or her security needs.

IATAC does not endorse any of the following product evaluations.

PACKET FILTERING

Cisco® Internetworking Operating System (IOS) Firewall

Abstract

The Cisco® IOS Firewall provides robust, integrated firewall and intrusion detection (ID) functionality for every perimeter of the network. Available for a wide range of Cisco IOS software based routers, the Cisco IOS Firewall offers sophisticated security and policy enforcement for connections within an organization (Intranet), between partner networks (Extranets), and for securing Internet connectivity for remote and branch offices.

A security-specific, value-added option for Cisco IOS Software, the Cisco IOS Firewall enhances existing Cisco IOS security capabilities, such as authentication, encryption, and failover, with state-of-the-art security features, such as stateful, application-based filtering (context-based access control) and defense against network attacks through user authentication and authorization and real-time alerts.

- **Flexibility**—all-in-one solution provides multi-protocol routing, perimeter security, intrusion detection, VPN functionality, and dynamic, per user authentication and authorization
- **Scalable Deployment**—scales to meet any network's bandwidth and performance requirements
- **Investment Protection**—leverages existing multi-protocol router investment
- **VPN Support**—provides a complete VPN solution based on Cisco IOS IPSec, and other CISCO IOS software-based technologies, including L2TP tunneling and Quality of Service (QoS)

Cisco IOS Firewall

Type of Firewall	Packet Filtering
OS	Self Contained
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Cisco
Availability	*http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_vrfaw.html*

Clavister® SW Software Series Firewalls

Abstract

The Clavister® SW Series is designed for users who require security technology on their own choice of hardware. Reasons for choosing a software solution may range from specific functional requirements, platform design, or simply because spare hardware is available.

Most important, a Clavister customer has the functionality required from a specific security solution. To suit market requirements, products are segmented within the Clavister SW Series. Orientation and choice based on functional requirements are therefore simplified. Without compromising on customization, a number of standard configurations are offered. The differences between models are performance and functionality, similar to the different products in the appliance series. Moreover, if requirements change, the product license can be easily upgraded to increase capacity and functionality.

Clavister SW Software Series Firewalls

Type of Firewall	Packet Filtering
OS	Self Contained
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Clavister
Availability	*http://www.clavister.com/products/security_software_overview.html*

fBuilder Lite and fBuilder Plus

Abstract

fBuilder is a Web-based utility for building and configuring your ipchains or iptables-based on Linux firewall. Written by the author of fwconfig, the fBuilder product line offers many new features that will meet the requirements of firewall creation. InnerTek Software currently offers two versions of fBuilder: fBuilder Lite, a free, ipchains-only version of fBuilder that includes a standard set of features; and fBuilder Plus, which includes edit, insert, and delete capabilities for firewall rules, automatic back traffic rule creation, log reporting, and export capabilities.

fBuilder products are also used for administering existing firewalls. When begun, fBuilder will detect a running firewall and permit it to save information to a file. From that point, the firewall may be modified with the expert add utility or by using the edit and insert capabilities of fBuilder Plus.

Its authors, InnerTek Software, LLC, commercially support fBuilder. All support is handled *via* email by sending a detailed description of the problem to *support@innertek.com*

fBuilder Lite and fBuilder Plus

Type of Firewall	Packet Filtering
OS	Linux
Hardware	
License	Freeware
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	InnerTek
Availability	*http://www.innertek.com/Software/fbuilder.shtml*

Firewall Builder for Linux and Windows®

Abstract

Firewall Builder is a graphical user interface (GUI) firewall configuration and management tool that supports iptables (netfilter), ipfilter, pf, Internet protocol firewall (IPFW), Cisco PIX (FWSM, ASA), and Cisco routers extended access lists. Both network administrators and hobbyists managing firewalls with policies more complex than is allowed by simple Web-based UI can simplify management tasks with the application. The program runs on Linux, FreeBSD, OpenBSD, Windows, and Mac OS X, and can manage both local and remote firewalls.

Firewall Builder permits managing multiple firewalls using the same network object database. A change made to an object is immediately reflected in the policy of all firewalls using this object. An administrator needs only to recompile and install policies on actual firewall machines.

In Firewall Builder, an administrator works with an abstraction of firewall policy and NAT rules; software effectively "hides" specifics of a particular target firewall platform and helps the administrator focus on implementing security policy. Back-end software components, or policy compilers, may deduct many parameters of policy rules using information available through network and service objects and therefore generate fairly complex code for the target firewall. This relieves an administrator from having to remember all its details and limitations. Policy compilers may also run sanity checks on firewall rules to ensure typical errors are caught before generated policy is deployed.

Firewall Builder for Linux and Windows

Type of Firewall	Packet Filtering
OS	Linux
Hardware	
License	Opensource
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	fwbuilder
Availability	*http://www.fwbuilder.org/archives/cat_about.html*

Alcatel-Lucent VPN Firewall

Abstract

The Alcatel-Lucent VPN Firewall Brick® portfolio offers a broad range of enterprise and carrier-class security solutions to protect corporate and service provider networks, as well as enable revenue-generating services for the carriers. The portfolio secures delivery of mission-critical IP applications to headquarter employees, branch offices, trading partners, road warriors, and customers.

Based on patented Bell-Labs technologies, the Alcatel-Lucent VPN Firewall Brick solutions offer unique capabilities to install invisibly to the IP infrastructure, for securing and guaranteeing quality of voice over Internet protocol (VoIP), for protecting Web-facing applications, and for remote management.

The Brick solutions are highly available, scalable, and geo-diverse, and secure many applications, including:

- Advanced security services
- Mobile data security
- Secure storage network secure solution
- Fine-grained bandwidth management capabilities (per rule and per session)
- VoIP Security Services for session initiation protocol (SIP), H.323, and Alcatel-Lucent OmniPCX-based solutions
- VPN services for site-to-site and remote access
- Secure data center Web and application hosting
- Packet data gateway and packet data interworking functions for dual-mode Wireless/Wireless Fidelity (WiFi) VPN and VoIP/data security
- W-CDMA Femto Base Station Router Security Services

The Alcatel-Lucent VPN Firewall includes the following—

- **VPN Firewall Bricks®**—Integrated firewall, VPN, QoS, Virtual Local Area Network (VLAN), and virtual firewall platforms
- **Alcatel-Lucent IPSec Client**—Secure remote access software for mobile workers
- **Alcatel-Lucent Security Management Server**—Carrier grade software to streamline security, VPN, and QoS provisioning and management

Alcatel-Lucent VPN Firewall

Type of Firewall	Packet Filtering
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	True
Common Criteria	Evaluation Assurance Level (EAL) 2
Developer	Lucent Technologies
Availability	*http://www.alcatel-lucent.com/wps/portal/products/detail?LMSG_CABINET=Solution_Product_Catalog&LMSG_CONTENT_FILE=Products/Product_Detail_000202.xml*

CIRCUIT LEVEL GATEWAY

ACTANE Controller

Abstract

ACTANE Controller is a comprehensive firewall aiming to satisfy high-level security policies, including packet filtering, circuit level gateway, and application proxies, including full simple network management protocol (SNMP) management and object oriented transparent proxying (OOTP), our unique technology. ACTANE Controller also supports token-based strong authentication algorithms.

The main design rules of ACTANE Controller are as follows—

- Anything not explicitly permitted is forbidden.
- User and application are transparent.
- Management is easy and coherent.
- The firewall model is a true security model.

ACTANE defined a high-level strategy to satisfy the following requirements in addition to security features—

- The firewall must be as easy as possible to use while remaining highly effective.
- Easy setup and easy management is necessary.
- As much as possible, it is necessary to use standardized protocols or those following a standardization process.
- The hardware architecture of the firewall is secure, upgradeable, and inexpensive.
- A fully SNMP manageable firewall must exist.

ACTANE Controller

Type of Firewall	Circuit Level Gateway
OS	Self-Contained
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	ACTANE
Availability	*http://www.actane.com/controll.htm*

BizGuardian® Firewall

Abstract

The BizGuardian® Firewall provides a reliable Unix Kernel, [Berkeley Software Distribution (FreeBSD)], customized in a highly secure, easy-to-install software appliance that may turn any old Pentium class computer into a high-performance firewall. The complexity of installing Unix and configuring a firewall is totally hidden behind the easy-to-use, browser-based administration. There is no operating system to install, backup, or configure, and BizGuardian includes automatic download and installs all necessary software.

BizGuardian stands between all servers and PCs on a network and the outside world. It provides a simple, inexpensive, plug-and-play firewall device to secure organizational assets.

Features

- **Automatic setup**—Permits novices to set up and use. Simply boot the BizGuardian floppy disk
- **Not a personal firewall**—Protects your entire network
- **Reduce network costs**—Shares a single IP address across all computers on your network
- **Scalability**—May grow to hundreds of users with little incremental cost
- **Rich product features**—Permit multiple users on a single Internet connection with high performance

BizGuardian Firewall

Type of Firewall	Circuit Level Gateway
OS	Self-Contained
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	BizGuardian
Availability	*http:/www.bizguardian.com/firewall.php*

Cequrux® Firewall

Abstract

The CEQURUX® Firewall is an intelligent, high-performance, software-based Internet firewall. It provides an extensive set of Internet services with a fine degree of access control and sophisticated graphical administration, accounting, and logging tools. Cequrux features include the following—

Features

- Completely transparent
- High-performance contextual gateway
- Application proxies
- Advanced ID
- Network address translation
- Demilitarized zone (DMZ) support
- Intelligent content management
- Extensive email handling
- Fine granularity access control
- Distributed and split domain name server (DNS)
- VPNs with strong cryptography
- Integrated post office protocol version 3 (POP3) and FTP and HTTP servers
- Secure internet control message protocol (ICMP) and UDP support
- Powerful Management GUI

Cequrux Firewall

Type of Firewall	Circuit Level Gateway
OS	Self-Contained
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Cequrux
Availability	

EGG Network Security Appliance (NSA)

Abstract

EGG NSA is a high-end network perimeter protection appliance with a secure, proprietary embedded operating system, stateful inspection firewall, IDS, VPN concentrator, DMZ support, and Webfilter.

EGG NSA employs systems that perform automatic updates of firmware, application software, and the IDS knowledge base. It offers an object-oriented administrative interface and advanced auditing and reporting and is also ready to connect to a SentryTM Queues and Delays at Roadworks (QUADRO) outsourcing platform for network security services.

EGG NSA (Network Security Appliance)

Type of Firewall	Circuit Level Gateway
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	QUADRO
Availability	*http://www.eggnsa.it/products/appliances.php*

Global Technology Associates (GTA) Firewall

Abstract

All GTA Firewall products are powered by GB OS, our proprietary operating system. GB OS is a totally self-contained system that integrates both an operating system and a hybrid firewall technology into a single, high-performance compact system.

GB OS is a comprehensive firewall system that prevents unauthorized access from untrusted networks, completely hides your internal network, and provides transparent network access to users on the protected hidden network. Available content filtering, antivirus, and anti-spam features extend the ability to manage these threats to a network's integrity. The system uses stateful packet inspection and application firewall techniques combined with a powerful network address translation system. GB OS provides a user with complete, transparent network access to external and private service networks for applications based on IP protocols (*e.g.,* TCP, UDP, and ICMP). The system also supports transparent network access for difficult application protocols such as *FTP,* RealPlayer, CU SeeMe, Apple Quicktime Streaming protocol, Microsoft Netmeeting, and real-time streaming protocol (RTSP) applications. The GB OS also includes a built-in IPSec VPN facility.

GTA Firewall

Type of Firewall	Circuit Level Gateway
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Global Technology Associates
Availability	*http://www.gta.com/firewalls/*

iptables

Abstract

netfilter.org is home to the software of the packet-filtering framework inside the Linux 2.4.x and 2.6.x kernel series. Software commonly associated with netfilter.org is iptables.

Features

Software inside this framework enables packet filtering, network address port translation (NAPT), and other packet mangling. It is the redesigned and heavily improved successor to the previous Linux 2.2.x ipchains and Linux 2.0.x ipfwadm systems.

netfilter is a set of hooks inside the Linux kernel that permits kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack.

Main Features

- Stateless packet filtering Internet Version 4 and Version 6 (IPv4 and IPv6)
- Stateful packet filtering (IPv4)
- All types of NAT and NAPT
- Flexible and extensible infrastructure
- Multiple layers of application programming interfaces (API) for third-party extensions
- Large number of plug-in and modules kept in 'patch o matic' repository

iptables

Type of Firewall	Circuit Level Gateway
OS	Self-Contained
Hardware	
License	Open source
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Netfilter
Availability	*http://www.netfilter.org*

Netgear® Business Wired VPN and Firewall Routers

Abstract

The NETGEAR® ProSafe® wired and wireless VPN solutions offer small and medium-sized businesses (SMB) a variety of security and remote access options. The ProSafe SSL VPN Concentrator sits behind the firewall and delivers secure, clientless, Web-based remote access.

NETGEAR's ProSafe business-class VPN Firewall routers deliver full network access between headquarters locations, remote/branch offices, and telecommuters. All-in-one devices offer stateful packet inspection (SPI) firewall, VPN intrusion detection/prevention, NAT, advanced encryption standard (AES) and triple data encryption standard (3DES) encryption, Denial of Service (DoS) protection, anti-spam policy enforcement (select models), content filtering and more.

Key Benefits

- ICSA certified, true firewall with SPI and ID
- DoS attack protection and VPN pass through
- Built-in print server and NAT routing
- Easy-to-use SmartWizard and install assistant
- FR114P printer compatibility list
- Ultimate security with true ICSA certified firewall

Netgear Business Wired VPN and Firewall Routers

Type of Firewall	Circuit Level Gateway
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Netgear
Availability	*http://www.netgear.com/Products/VPNandSSL.aspx*

BorderManager®

Abstract

Novell BorderManager® includes firewall and VPN technologies that protect networks and resources while ensuring end user productivity.

Features

From firewall and VPN functionality to Internet access control and content filtering, Novell BorderManager offers an array of features to protect a network and its resources. Specifically, Novell BorderManager does the following—

- Secures remote access to network resources
- Provides VPN services based on Secure Internet Protocol (IPsec)
- Works with IPsec certified products
- Supports open standards, including Lightweight Directory Access protocol (LDAP)
- Supports advanced authentication
- Offers browser-based administration
- Includes Novell Client Firewall 2.0
- Supports key content filtering solutions
- Provides firewall services certified by ICSA Labs
- Leverages Novell International Cryptography Infrastructure (NICI), an encryption engine validated by Federal Information Processing Standard (FIPS) 140

BorderManager

Type of Firewall	Application Level
OS	NetWare 6.5 SP 6 or later, or Novell Open Enterprise Server SP 2 or later
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Novell
Availability	*http://www.novell.com/products/bordermanager*

Fortinet® FortiGate®

Abstract

Fortinet® firewall technology combines application-specific integrated circuit (ASIC)-accelerated stateful inspection with integrated application security engines to quickly identify and block complex threats. FortiGate® firewall protection integrates with other key security features such as VPN, antivirus, intrusion prevention system (IPS), Web filtering, anti-spam, and traffic shaping to deliver multi-layered security that scales from SOHO/ROBO appliances to multi-gigabit core network or data center platforms. FortiManager™ and FortiAnalyzer™ turn-key appliances provide centralized management of thousands of FortiGate systems and detailed reporting capabilities for internal auditing and reporting.

Features

- FortiASIC™ network processors enable firewall and traffic shaping at wire speeds in selected FortiGate platforms.
- Full integration with other Fortinet security technologies (*e.g.,* antivirus, Web filtering) enables extensive protection profiles for in-depth defense.
- Virtual security domains and security zones enable network segmentation by customer, business unit, or any other physical or logical division for increased policy granularity and multi-layered security.
- Three operational modes (transparent, static NAT, and dynamic NAT) adapt to existing infrastructure for deployment versatility.
- Easily customized application definitions deliver additional policy granularity for more accurate protection.
- FortiClient end-point security agents extend firewall protection to remote desktop computers, mobile laptops, and smartphones that operate outside the network perimeter.
- H.323, SIP, and SCCP protocol support to protect VoIP services.
- Support for dynamic routing protocols (routing information protocol [RIP], open shortest path first [OSPF], border gateway protocol [BGP] and PIM) required in complex enterprise network environments.
- High-availability support for uninterrupted service.
- Available centralized management and reporting reduce capital and operational expenditures for firewall protection.

Fortinet FortiGate

Type of Firewall	Application Level
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	EAL 4
Developer	Fortinet
Availability	*http://www.fortinet.com/solutions/firewall.html*

HotBrick® SoHo 401 VPN

Abstract

The SoHo 401 VPN is a solution to protect a network from external threats (*e.g.,* hackers, invasions) while providing safe VPN connections to remote networks. HotBrick® CF401VPN permits the definition of access policies with user division into groups with distinct Internet access and policies. The SoHo 401 VPN is a firewall, a high-bandwidth router, and a four-port switch that may connect securely to remote networks through VPN tunnels. It has NAT, SPI, and anti-DoS features and provides attack alerts *via* email.

HotBrick SoHo 401 VPN

Type of Firewall	Application Level
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	HotBrick
Availability	*http://www.hotbrick.com/cf401vpn.asp*

The SoHo 401 VPN permits users to perform the following—

- Create separate user control profiles for each member.
- Control which Internet applications a user is permitted to use.
- Block objectionable content based on a user's maturity level.
- Time of Day—You may set rules to enforce when a user is permitted to access the Internet.
- Daily Access Permittance—You may set daily allotments to manage how much time each user is permitted to spend on the Internet on any given day of the week.
- Blocking Access—You may block a user's access to certain online applications such as Web, email, chat rooms, peer to peer applications, and online games.
- Filtering—You may filter out objectionable Web content by selecting different content categories.

Internet Security and Acceleration (ISA) Server 2006

Abstract

Microsoft® Internet Security and Acceleration (ISA) Server 2006 is an integrated network edge security gateway that helps protect IT environments from Internet-based threats while providing users fast and secure remote access to applications and data. ISA Server 2006 is available in two versions: Standard Edition and Enterprise Edition.

ISA Server contains a full-featured, application-layer-aware firewall that helps protect organizations of all sizes from attack by both external and internal threats. ISA Server performs deep inspection of Internet protocols such as *HTTP,* which enables it to detect many threats that traditional firewalls cannot. The integrated firewall and VPN architecture of ISA Server support stateful filtering and inspection of all VPN traffic. The firewall also provides VPN client inspection for quarantine solutions based on Microsoft Windows Server 2003, thus helping protect networks from attacks that enter through a VPN connection. A completely new user interface, wizards, templates, and management tools also help administrators avoid common security configuration errors.

Internet Security and Acceleration (ISA) Server 2006

Type of Firewall	Application Level
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	EAL 4+
Developer	Microsoft
Availability	*http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/overview.aspx*

Juniper Networks Firewall and IPsec VPN

Abstract

The Juniper Networks Firewall and IPsec VPN security devices combine a stateful inspection firewall with Deep Inspection technology for application-level protection, IPsec VPN capabilities, and DoS mitigation functions. The devices are also manageable by a policy-based central management system, NetScreen Security Manager, and are available to meet the throughput requirements of enterprises of all sizes.

Features

- Strong firewall security for access control, user authentication, and network and application-level attack protection
- Lower capital investment, support, deployment, and operations costs for overall lower total cost of ownership (TCO)
- Predictable performance for a highly reliable, available, and secure network
- Integrated security devices with stateful and deep inspection firewall, IPsec VPN, antivirus, and Web filtering
- Rapid deployment to quickly get a new device up and running
- Device redundancy and resiliency for high availability
- Secure wireless access for enterprise remote offices
- DoS attack protection
- Application-level security with deep inspection and Web filtering
- Transparent mode to drop device into existing network with minimal changes
- Dynamic routing support to reduce reliance on manual intervention

Juniper Networks Firewall and IPsec VPN

Type of Firewall	Application Level
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	True
Common Criteria	EAL 4
Developer	Juniper
Availability	*http://www.juniper.net/us/en/products-services/security/*

Kerio® WinRoute® Firewall

Abstract

Kerio® WinRoute® Firewall defends against external attacks and viruses and may restrict access to Web sites based on their content.

Features

- Deep inspection firewall
- VPN, VPN Client, and Secure Socket Layer (SSL) VPN
- Antivirus gateway protection
- Surf protection
- Content filtering
- User specific access management
- Fast Internet sharing
- VoIP and Universal Plug and Play (UPnP) support
- Internet monitoring
- Administration, alerts, and statistics

Kerio WinRoute Firewall

Type of Firewall	Application Level
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Kerio
Availability	*http://www.kerio.com/firewall*

PORTUS Application Protection System (APS) and Firewall for Linux

Abstract

The PORTUS Application Protection System (APS) functions as an in-line Network Intrusion Prevention System (NIPS) and firewall. PORTUS delivers in-depth protection against known and unknown forms of attack. Protocol Anomaly Detection (PAD) detects and blocks previously unknown forms of attack without requiring signatures. Stateful Signature Analysis (SSA) of the payload data permits detection and blocking of known attacks. Both the PAD and SSA may be fine-tuned to unique applications to provide the highest level of security without producing false alarms. The PORTUS APS can stop all forms of attack in real time and prevent them from reaching protected systems.

PORTUS APS and Firewall Linux

Type of Firewall	Application Level
OS	Unix
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Livermore Software Laboratory, Intl.
Availability	*http://www.lsli.com/portus.html*

Main Technologies (See PORTUS APS and Firewall Solaris for additional technologies offered.)

- Application specific proxies for email, *FTP, HTTP,* terminal services (telnet, TN3270)
- Real audio and real video, RTSP
- Advanced application proxy
- API
- Perl Compatible Regular Expressions (PCRE)
- Pattern matching
- Remote procedure call (RPC) and UDP proxy
- Integrated interoperable VPN support
- Hardware-assisted encryption feature available
- Socks V4 & V5 proxy
- Email controls

PORTUS APS and Firewall for Solaris

Abstract

The PORTUS APS Appliance provides tuned, pre installed PORTUS software on a hardware platform. This solution provides easy installation of an appliance without its inherent limitations. Multiple configurations are available to match the performance and availability requirements of a site.

Main Technologies (See PORTUS APS and Firewall Linux for additional technologies offered.)

- Integrated content filtering (Universal Resource Locator [URL], Java, JavaScript, ActiveX, Spam)
- Fault Tolerant High Availability (99.999%) Option
- Integrated workload balancing
- High-speed Web caching
- Dual DNS
- Intrusion monitoring and detection
- GUI
- Network and host security scanners
- Built-in monitors for detecting attacks, checking system, and network integrity
- Real-time performance monitor
- Extensive auditing with report programs that generate more than 57 unique reports
- Automated operations with log rotation and archiving

PORTUS APS and Firewall Solaris

Type of Firewall	Application Level
OS	Unix
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Livermore Software Laboratory, Intl.
Availability	*http://www.lsli.com/portus.html*

SteelGate

Abstract

SteelGate is a high-performance VPN firewall appliance that enables organizations to prevent attacks and block malicious behavior, control both inbound and outbound network traffic, and centrally manage the perimeter defense infrastructure in a single security solution. SteelGate is a comprehensive firewall appliance that is based on the Common Criteria certified BorderWare Firewall Server™ software.

SteelGate has default settings and a simple interface that protects against misconfiguration, a common source of vulnerability, while permitting IT administrators to get up and running faster. By tracking multiple threat types in real time, SteelGate makes a more informed and accurate decision about network traffic.

SteelGate

Type of Firewall	Application Level
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	EAL 4+
Developer	Borderware
Availability	*http://www.borderware.com/products/borderware_steel_gate.php*

Features

- Network attacks
- Buffer overflow prevention
- Antivirus
- Anti spyware
- Integrated NAT
- Superior protection with application-level proxies

Zorp Modular Application Level Gateway

Abstract

The Zorp architecture contains several functional entities that may be deployed either in individual devices or onto a single device—

- Zorp application level gateways and firewalls
- Zorp Management System
- Zorp Authentication System
- Zorp Management Console

Hardened Operating System

- Quick and easy installation
- Strong and effective security solutions require especially "hardened" system software to ensure a high level of security, stability, and interoperability that cannot be reached using conventional OS software
- Based on a Balabit-hardened Linux (Debian Gnu's Not Unix [GNU] and Linux) distribution.

The Zorp Application Level Gateway and Firewall

Zorp is a security solution designed to give total control over all network traffic. Thanks to its modular nature, Zorp is capable of analyzing all popular protocols and embedded data streams on the application layer. Zorp offers additional features, including networking functions, authentication, a VPN gateway, a stripped-down highly secure operating system, and support for various authentication solutions such as public key cryptography.

Zorp Modular Application Level Gateway

Type of Firewall	Application Level
OS	Self-Contained
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	BalaBit
Availability	*http://www.balabit.com/products/zorp*

Barracuda® Web Application Firewall

Abstract

The Barracuda® Web Application Firewall protects Web applications and Web services from malicious attacks, and can also increase the performance and scalability of these applications. The Barracuda Web Application Firewall offers a capability needed to deliver, secure, and manage enterprise Web applications from a single appliance through an intuitive, real-time user interface.

- Single point of protection for inbound and outbound traffic for all Web applications
- Protects Web sites and Web applications against application layer attacks
- Delivers best practices security right out of the box
- Monitors traffic and provides reports about attackers and attack attempts

Barracuda Web Application Firewall

Type of Firewall	Stateful Inspection
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Barracuda
Availability	*http://www.barracudanetworks.com/ns/products/web-site-firewall-overview.php*

Cisco ASA 5500 Series

Abstract

The Cisco ASA 5500 Series Firewall Edition enables businesses to securely deploy mission-critical applications and networks in a highly reliable manner. Businesses can protect their networks from unauthorized access using the Cisco ASA 5500 Series Firewall Edition's robust policy enforcement services. These services combine with VPN services to enable businesses to securely extend their networks across Internet connections to business partners, remote sites, and mobile workers. This flexible solution can adapt as an organization's needs evolve along with the ever-changing security threat landscape, giving businesses the ability to easily integrate intrusion prevention, antivirus, anti-spam, anti-spyware, URL filtering, and other advanced content security services for additional layers of protection.

Capabilities of the Cisco ASA 5500 Series Firewall Edition include:

- **Trusted and deployed firewall technology**—Building upon the capabilities of the Cisco PIX® Family of security appliances, the Cisco ASA 5500 Series provides a wide range of services to secure modern network environments. Flexible policy capabilities prevent unauthorized access to network resources or vital corporate information. Advanced application control capabilities help businesses effectively control the use of peer-to-peer file sharing, instant messaging, and other non-corporate applications.
- **Threat-protected VPN**—Building upon the VPN capabilities of the Cisco VPN 3000 Series Concentrator, the Cisco ASA 5500 Series Firewall Edition provides secure site-to-site and remote-user access to corporate networks and services. This solution offers businesses flexibility for secure connectivity by combining support for SSL and Ipsec VPN capabilities into a single solution. Using the services offered by the Cisco ASA 5500 Series Firewall Edition, businesses can enforce identity-based security and networking policies to all network traffic, thus enabling businesses to tailor-fit access privileges for every group of employees, contractors, and business partners.
- **Adaptive design provides investment protection and extensibility to address future threats**—The Cisco ASA 5500 Series Firewall Edition can adapt as business needs change through its modular design. One can easily expand the number of security services offered by adding a high-performance, purpose-built Cisco ASA 5500 Series security services module, such as the Advanced Inspection and Prevention Security Services Module for advanced intrusion prevention services, or the Content Security and Control Security Services Module for advanced antivirus, anti-spam, and other content security services.
- **Intelligent network integration and enterprise-class resiliency**—The Cisco ASA 5500 Series Firewall Edition delivers a wide range of intelligent networking services for seamless integration into today's diverse network environments. One can maximize network uptime and throughput by taking advantage of the many resiliency and scalability services this solution has to offer, such as Active/Active high availability, "zero-downtime software upgrades," and integrated VPN clustering and load balancing.
- **Easy deployment and management**—The Cisco management and monitoring suite enables large-scale deployment and operation of the Cisco ASA 5500 Series Firewall Edition. Cisco provides a solution covering management and monitoring. Also included with the solution is Cisco Adaptive Security Device Manager, which provides a powerful, yet easy-to-use browser-based management and monitoring interface for individual security appliances.

Models

- ASA 5505 Base/Security Plus
- ASA 5510 Base/Security Plus
- ASA 5520, 5540, 5550, 5580-20, 5580-40

Cisco ASA 5500 Series

Type of Firewall	Stateful Inspection
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	EAL 4
Developer	Cisco
Availability	*http://www.cisco.com/en/US/products/ps6120/index.html*

ETM System

Abstract

The ETM System hosts a Voice Firewall solution and delivers an integrated set of powerful applications to secure, optimize, and efficiently manage a voice network and communications. The solutions work independently of the Private Branch Exchange (PBX) across any mix of multi-vendor legacy and VoIP systems in a network and scale to support small site operations as well as the largest multinational corporations.

The ETM System contains hardware and software. ETM platform appliances sit inline, at the edge of a voice network between a PBX and the central office, covering all VoIP and telephone directory monitor (TDM) voice circuits. Every inbound and outbound call is logged by the system, checked against voice network security access and usage policies, and monitored for call quality and performance.

The ETM System application product suite includes—

- Voice Firewall Icon
- Usage Manager
- Performance Manager
- Voice IPS
- Call Recorder

ETM System

Type of Firewall	Stateful Inspection
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	EAL 2
Developer	SecureLogix
Availability	*http://www.securelogix.com/products/etm_overview.htm*

Fireware® XTM Pro

Abstract

Fireware® XTM Pro is the advanced operating system that ships with all WatchGuard XTM 1050 security appliances. It offers enhanced networking capabilities to keep high-volume traffic flowing smoothly, with maximum uptime. This firewall maintains high availability, session sync, fast failover, and the following features—

- Application-layer content inspection recognizes and blocks threats stateful packet firewalls cannot detect.
- Wide-ranging protection comes from robust security on *HTTP, HTTPS, FTP,* SMTP, POP3, DNS, and TCP/UDP.
- Security subscriptions boost protection in critical attack areas for unified threat management.
- Integrated SSL VPN provides simple, anywhere-anytime network access.

Firebox XTM Pro

Type of Firewall	Stateful Inspection
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	EAL 4 in process
Developer	WatchGuard
Availability	*http://www.watchguard.com/products/xtm-1050/index.asp*

Ingate® Firewall

Abstract

Ingate® Firewalls are SIP-capable firewalls for enterprises that want access to SIP-based communications such as presence, instant messaging, audio and video conferencing, and VoIP. Ingate products include a SIP proxy and a SIP registrar, support NAT and Port Address Translation (PAT), and have Transport Layer Security (TLS) support for encrypted SIP signaling—which means that instant messages are automatically encrypted. Ingate has a SIP-capable firewall that passed system integration testing with WorldCom, CommWorks, and Broadsoft.

Features

- Firewall comes complete with hardware and software
- Easy to install and configure
- Alarm and advanced logging
- Proxy at TCP and UDP levels, application-level gateway for FTP traffic
- User authentication using RADIUS
- Adapted for remote administration
- SIP support for VoIP and other person-to-person applications
- VPN module including support for IPsec
- Optional SIP Trunking module for connecting an IP-PBX to a service providers SIP trunk
- Optional QoS module for bandwidth limitation and traffic prioritizing
- Optional Remote SIP Connectivity module for connecting remote users
- Optional VoIP Survival module provides VoIP redundancy if connection fails
- Optional Advanced SIP Routing module gives flexible routing functions for SIP traffic

Ingate Firewall

Type of Firewall	Stateful Inspection
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Ingate
Availability	*http://www.ingate.com/firewalls.php*

McAfee Firewall Enterprise (Sidewinder)

Abstract

McAfee Firewall Enterprise advanced capabilities, such as reputation-based global intelligence, configurable application-level protection, encrypted traffic inspection, intrusion prevention, antivirus, and content filtering to block attacks before they occur.

Firewall Enterprise is easy to administer with centralized firewall management and reporting and user-friendly rule-creation capabilities. Three additional products simplify management and help a user respond more quickly—

McAfee Firewall Profiler (sold separately) takes a feed from McAfee Firewall Enterprise and instantly analyzes this information to provide visibility into how firewall rules interact with and impact the network. Profiler dramatically reduces the time needed to solve firewall-related network or application outages from hours to minutes, turning substantial manual efforts into a few simple clicks.

- McAfee Firewall Reporter (included) turns audit streams into actionable information. This security event management (SEM) tool delivers central monitoring plus correlated alerting and reporting to help meet major regulatory requirements, including PCI DSS, Gramm-Leach-Bliley Act of 1999, HIPAA, SOX, and FISMA.

McAfee Firewall Enterprise Control Center, sold separately, offers centralized firewall policy management for multiple Firewall Enterprise appliances.

McAfee Firewall Enterprise

Type of Firewall	Stateful Inspection
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	True
Common Criteria	EAL 4
Developer	Secure Computing
Availability	*http://www.securecomputing.com/index.cfm?skey=232*

Nortel Switched Firewalls

Abstract

The Switched Firewall Portfolio provides enterprise class stateful firewall protection. This portfolio is made up of the Switched Firewall products that protect network applications, services and multimedia (VoIP and video) applications from hackers, attacks, worms, and viruses in IT data centers, service provider networks, and hosting infrastructures.

The Switched Firewall, based on Check Point Firewall-1 technology, also leverages Check Point Secure XL technology for high-performance acceleration. The Switched Firewall delivers 99.999% availability and expertise and support for deployment into business-critical next generation networks.

Nortel Switched Firewalls

Type of Firewall	Stateful Inspection
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	EAL 4
Developer	Nortel
Availability	*http://products.nortel.com/go/product_*content.jsp?segId=0&parId=0&prod_id=36220&locale=en-US

NS200 Internet Security Server

Abstract

NetSentron® NS200 Server is a stand-alone security appliance that provides a simple and secure method of keeping a network safe. At the same time, it provides the ability to connect remote users to a corporate network, content filtering for safe Web surfing, and spam filtering. The server is built using field-tested security technology and is also available in rack mount (NS200R).

Features

- Stand-alone appliance (software installation not required)
- Firewall with IDS
- Content filtering
- Remote access (VPN)
- Spam filter
- Pop-up blocker

NS200 Internet Security Server

Type of Firewall	Stateful Inspection
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	NetSentron
Availability	*http://www.netsentron.com/servers.html*

NS200 Software

Abstract

NetSentron NS200PRO provides Internet security solutions for SMBs and educational Internet users. The NetSentron is used for Firewall protection, for preventing access to inappropriate Internet sites, for managing remote offices, and much more.

Once installed, you can use the Web-based administrative interface to configure the NetSentron to your business, school, and/or personal Internet security requirements.

NetSentron uses a Linux-based operating system and is designed to be installed on a separate machine.

NS200 Software

Type of Firewall	Stateful Inspection
OS	Self-Contained
Hardware	Required
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	NetSentron
Availability	*http://www.netsentron.com/products.html*

Features

- Intelligent content filtering
- High-level firewall protection
- IDS
- VPN capabilities (Secure remote access to other offices or schools)
- SPAM filtering

SmoothWall® Express

Abstract

SmoothWall® Express is an open-source firewall distribution based on the GNU and Linux operating system. Linux is secure, highly configurable, and freely available as open source code. SmoothWall includes a hardened subset of the GNU and Linux operating system, so there is no separate OS to install. Designed for ease of use, SmoothWall is configured *via* a Web-based GUI and requires absolutely no knowledge of Linux to install or use.

A range of add-on modules provides extra functionality, such as Web content filtering, VPN gateway, and QoS.

SmoothWall Express

Type of Firewall	Stateful Inspection
OS	Self-Contained
Hardware	Required
License	Open source
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Smoothwall
Availability	*http://www.smoothwall.org*

SteelGate

Abstract

SteelGate is a high-performance VPN firewall appliance that enables organizations to prevent attacks and block malicious behavior, control both inbound and outbound network traffic, and centrally manage the perimeter defense infrastructure in a single security solution. SteelGate is a comprehensive firewall appliance that is based on the Common Criteria certified BorderWare Firewall Server TM software.

SteelGate has powerful default settings and a simple interface that protects against misconfiguration, a common source of vulnerability, while permitting IT administrators to get up and running faster. By tracking multiple threat types in real time, SteelGate makes an informed and accurate decision about network traffic.

Features

- Network attacks
- Buffer overflow prevention
- Antivirus
- Anti-spyware
- Integrated NAT
- Superior protection with application-level proxies

SteelGate	
Type of Firewall	Application Level
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	EAL 4+
Developer	Borderware
Availability	*http://www.borderware.com/products/borderware_steel_gate.php*

StoneGate Firewall/VPN Appliance

Abstract

The StoneGate Firewall/VPN Appliance series delivers a different architecture, providing a different degree of network security and business continuity.

Features

- Set up a clustered, load balanced environment out of the box without third-party solutions.
- Drop-in Firewall Clustering Technology permits you to "drop" a cluster into the network environment without reconfiguring existing switches or routers.
- Stonesoft's patented Multi Link Technology enables a single or clustered StoneGate firewall to access multiple Internet and VPN connections across multiple Internet service providers (ISP), leased lines, or other connections.
- Server load sharing and health monitoring intelligence for server pools ensures availability and performance of business services.
- Multi-link VPN adds fault tolerance and transparent failover to VPN tunnels and VPN client connections.
- StoneGate Management Center makes the everyday management and configuration of StoneGate products easy.
- Log and alert browsing give an administrator a comprehensive overview of a security event while the built-in reporting tool draws an overview on what has been going on in the network.
- Multi Layer Inspection permits the firewall to act as a packet filter, performing stateful inspection or application-level firewall.

StoneGate Firewall/VPN Appliance

Type of Firewall	Stateful Inspection
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	True
Common Criteria	EAL 4+
Developer	Stonesoft
Availability	*http://www.stonesoft.com/en/products_and_solutions/products/fw/appliances/*

StoneGate Virtual Firewall/VPN Appliance

Abstract

StoneGate Virtual Firewall/VPN Appliance is an easy-to-add network firewall appliance for virtual environments.

StoneGate Virtual Firewall/VPN Appliances can be managed with StoneGate Management Center. The StoneGate Management Center offers unified management for all StoneGate Security appliances, both virtual and physical. The corporate security policy can be consistently enforced throughout the whole network.

Features

- One management platform for both physical and virtual environments, leveraging the power of the StoneGate Management Center
- Ensured secure, resilient, optimized connectivity with patented Stonesoft technologies
- Certified for the VMware™ ESX platform and supports VMsafe™ technology
- Support for a wide range of architectures and virtual platforms

StoneGate Virtual Firewall/VPN Appliance

Type of Firewall	Stateful Inspection
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	
Common Criteria	
Developer	Stonesoft
Availability	*http://www.stonesoft.com/en/products_and_solutions/products/fw/virtual_firewall/*

Check Point Power-1 and Blades

Abstract

Check Point appliances deliver powerful turnkey systems for deploying and managing Check Point's software solutions to address security needs. All Check Point appliances are built around a unified security architecture, enabling organizations to perform security management *via* a single, unified console. Check Point appliances now support a new Software Blades Architecture that provides flexible and fast deployment of security services without the addition of new hardware.

Power-1 appliances examine hundreds of applications, protocols, and services out of the box. As new applications and network-layer threats appear, Power-1 appliances can be updated with the latest protections and expanded with additional Software Blades to add more security capabilities. Power-1 is managed from the Check Point management servers, enabling you to centrally manage security policy for all sites through a single management console.

Check Point's Software Blade architecture enables organizations to efficiently tailor targeted managed solutions that meet targeted business security needs. All solutions are centrally managed through a single console that reduces complexity and operational overhead. And as new threats emerge, Check Point's Software blade architecture quickly and flexibly expands services as needed without the addition of new hardware or management complexity. Security gateway blades available are—

- Firewall
- IPSEC VPN
- IPS
- Web security
- URL filtering
- Antivirus and anti-malware
- Anti-Spam and email security
- Advanced networking
- Acceleration and clustering
- VoIP

Key Benefits

- Ensures availability of business-critical applications with up to 25 Gbps of firewall throughput and total system performance (Firewall + IPS) of up to 15 Gbps
- Field upgradeable for maximum performance flexibility (Power-1 11000 Series)
- Provides a comprehensive set of security Software Blades that is extensible on demand to include Web security, antivirus, anti-spyware, and anti-spam
- Simplifies administration with a single management console for all sites
- Protects against emerging threats with Software Blade update services

Check Point Power-1 and Blades

Type of Firewall	Security Suite
OS	Self-Contained
Hardware	Required
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	EAL 4
Developer	Check Point
Availability	*http://www.checkpoint.com/products/power-1/index.html*

Clavister Series Firewalls

Abstract

All Clavister Security Gateway Appliance series are Unified Threat Defense (UTD) compliant and are emphasizing high-performance firewall and VPN throughput with an easy-to-use, central, enterprise management system. The Security Gateway Appliances ranges from powerful carrier class products to small units for remote sites and branch offices. All Clavister appliances have the option to be used only as Firewall and VPN gateways or to also include ID and prevention system and antivirus functionality.

Clavister offers a comprehensive portfolio of Security Gateway appliances and related services. Important parameters in all Security Gateway appliances are carrier class level security, performance, and reliability.

Clavister SG Appliance Series Firewalls

Type of Firewall	Security Suite
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Clavister
Availability	*http://www.clavister.com/products/appliance_overview.html*

InJoy Firewall Linux, OS/2 and Windows

Abstract

The InJoy Firewall is a flexible firewall security solution for organizations of all sizes. It offers enterprise class, next generation security; preconfigured policy templates, including full customization options; seamless IPsec VPN integration; gateway capability; intuitive management; access control; a wealth of documented deployment examples; and comprehensive documentation.

Features

- Multiple operating system support
- License type of firewalls
- Customizable GUI
- Superior protection
- Access management
- Traffic shaping
- IPsec VPN support
- Gateway capability
- Multiple access technologies

InJoy Firewall Linux and Windows

Type of Firewall	Security Suite
OS	Linux, OS/2 and Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	F/X Communications
Availability	*http://www.fx.dk/firewall*

McAfee Unified Threat Management (UTM) Firewall (Formerly SnapGear)

Abstract

McAfee Unified Threat Management (UTM) Firewall is a complete office network-in-a-box Internet security appliance for SMBs. It features wide-area networking tools.

The UTM Firewall can easily set up an office with—

- A local network of office PCs (wired or wireless, including DHCP and all local area network (LAN)-routing functions)
- Secure connectivity to the Internet with Web-based content filtering
- Seamless LAN to wide area network (WAN) connectivity with secure remote VPN access for your branch offices and mobile staff
- A complete perimeter security solution, with options such as firewall, VPN, IDS/IPS, anti-spam, and content filtering

UTM works by converging all networking, firewall, intrusion prevention security, and remote access requirements into one high-speed, highly reliable, small-form-factor appliance.

The UTM Firewall has models ranging from entry-level SOHO appliance, to a rack mount unit intended for larger offices. No additional routers, switches, DHCP servers, wireless devices, or failover devices are needed.

All UTM Firewalls can be centrally managed *via* the McAfee UTM Firewall Control Center. Centralized management is critical to larger distributed environments—it allows network administrators to manage hundreds or even thousands of UTM Firewall appliances with a click of the mouse, including upgrades, policy changes, and other configuration tasks.

McAffee UTM Firewall

Type of Firewall	Security Suite
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	True
Common Criteria	EAL 4
Developer	Cyberguard Corporation
Availability	*http://www.mcafee.com/us/enterprise/products/network_security/utm_firewall.html*

NETASQ Firewall Appliance

Abstract

NETASQ appliances have been inspired by the UTM concept, and as such, integrate into all its appliances all the security functions that meet the needs of service providers, remote users, and businesses of all sizes.

- Real-time intrusion prevention
- Network and application firewall
- SSL VPN
- IPSEC VPN
- Advanced content filtering
- PKI
- SSO Authentication
- Bandwidth management

The core of the NETASQ Firewall U Series centers on its proprietary system that embeds firewall features and real-time intrusion prevention. The NETASQ engine analyzes network protocols in order to detect and block threats, and thanks to numerous behavioral analyses and different targeted signature databases (depending on the context), it delivers a very high level of security by dramatically reducing the risk of false alarms.

Firewall Monitor is a tool in the NETASQ Administration Suite that enables monitoring NETASQ UTM appliances in real time. Other functions such as configuration, updates, and reporting are conducted by the other tools in the suite. Firewall Monitor's user-friendly and easy-to-use graphical interface ensures advanced monitoring of NETASQ appliances.

NETASQ Firewall Appliance

Type of Firewall	Security Suite
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	NETASQ
Availability	*http://www.netasq.com/en/firewall/firewall-comparative.php*

PowerElf II

Abstract

The PowerElf II server appliance is a multi-function server appliance solution for SMBs and schools.

Server appliance features include anti-spam and antivirus protection, Internet sharing, Web and email server services, advanced file and print services, Auto Defense firewall technology, VPN, intrusion detection, remote administration, and many other functions in a preconfigured package.

Greencomputer's Auto Defense firewall technology helps to reduce the number of DoS and hacks because it may modify the firewall when it senses an attack.

- **Stateful Packet Filtering (SPF) Firewall**—Protects private data while giving users full Internet access. NAT hides an internal network from the Internet, giving additional protection from hackers. With new SSH remote access, system administrators will be able to securely connect to their PowerElf II Firewall Appliance without fear of hackers or snoops. Encrypted passwords, secure key authentication, and root logins may all be enabled or disabled easily from the Web-based GUI Interface.
- **IDS**—IDS monitors all incoming traffic on the PowerElf II security appliance, looking for suspicious or malicious traffic. If this type of traffic is detected, it is logged, blocked, and an alert message is sent to the administrator. The reports are viewable through the Web manager interface. If any of the data matches the rulesets that is used by the IDS, then it creates an alert.

PowerElf II

Type of Firewall	Security Suite
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Green Computer
Availability	*http://www.greencomputer.com/products/powerelf2*

SonicWALL® Firewall and VPN Appliances

Abstract

The SonicWALL® family of Internet security includes an ICSA-certified deep packet inspection firewall, IPsec VPN for remote access, IP address management features, and support for SonicWALL value-added security services.

The TZ Series is designed for SMBs as well as distributed enterprises with remote and branch offices. The TZ Series consists of the SonicWALL TZ 180, TZ 190, and TZ 210 appliances, which provide security, high-speed IPsec and SSL VPN technologies, and optional 802.11b/g/n wireless and optional 3G wireless broadband.

The PRO Series combines multiple network and security functions, including a deep packet inspection firewall, IPsec VPN, layered antivirus, anti-spyware, intrusion prevention, and Web content filtering capabilities into a single integrated appliance. Based on a dynamically updateable platform, PRO Series appliances are automatically updated to ensure zero day protection against a variety of network and application threats. Optimized for advanced networking and reliable operation, they are designed for mission-critical data and network communication deployments. At the core of every PRO Series appliance is SonicOS, SonicWALL's operating system, which provides policy-based firewall management over complex deployments and enables complete control over network traffic and application usage. The PRO Series delivers performance for organizations of all sizes, including branch offices, central sites, distributed enterprises, and data centers.

Selected Features & Benefits

- Re-assembly free deep packet inspection engine eliminates threats over unlimited file sizes and unrestricted concurrent connections, offering scalability.
- Real-time gateway antivirus, anti-spyware, anti-spam, and intrusion prevention capabilities secure the network against a comprehensive array of dynamic threats, including viruses, spyware, worms, Trojans, phishing attacks, and software vulnerabilities such as buffer overflows.
- SonicWALL Clean VPN™ deep packet inspection architecture assures mobile user connections and branch office traffic are decontaminated to prevent vulnerabilities and malicious code from being introduced into the corporate network from remote connections.
- Comprehensive application control prevents non-business traffic such as peer-to-peer and instant messaging applications at the administrator's discretion.
- Stateful high availability and load balancing features maximize total network bandwidth and maintain network uptime, ensuring uninterrupted access to critical resources.
- Standards-based VoIP capabilities provide security for every element of the VoIP infrastructure, from communications equipment to VoIP-ready devices such as SIP Proxies, H.323 Gatekeepers and Call Servers.
- Secure distributed wireless LAN services enable the appliance to function as a secure wireless switch and controller that automatically detects and configures SonicPoints™, SonicWALL wireless access points, for secure remote access in distributed network environments.
- Onboard QoS features use industry standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators to provide flexible bandwidth management for Voice over IP, multimedia content and business critical applications.
- Advanced security and networking features include 802.1q VLANs, enterprise routing support, WAN/WAN failover, zone and object-based management, inbound and outbound load balancing, advanced NAT modes, and more, providing granular configuration.

SonicWALLFirewall and VPN Appliances

Type of Firewall	Security Suite
OS	Self-Contained
Hardware	Included
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	SonicWALL
Availability	*http://www.sonicwall.com*

Armor2net Personal Firewall 3.12

Abstract

Armor2net personal firewall software stops hackers and data thieves and protects a PC from Internet-borne threats.

This firewall monitors all Internet connections to and from a computer to ensure that only legitimate traffic is permitted and alerts to attempted intrusions. You have the option to grant and deny access to the Internet on a per application basis, thus preventing worm, Trojan horse, and spyware programs from hurting a computer.

Features

- Armor2net firewall shows currently active connections and the details of these connections. With this personal firewall, you may shut off any unsafe connection and block the dangerous Internet sites.
- With its pop-up stopper, Armor2net stops browsers' pop-up ads windows. You may also customize the stopper on each individual Web site.
- The spyware remover detects your memory, registry, and hard drives for known spyware components and removes spywares safely.
- Armor2net is intelligent firewall software. Many actions will be automatically processed, thus freeing you from tedious and trivial operations

This tool has not been updated since Version 3.12, possibly indicating a lack of updates or a discontinuation of the tool.

Armor2net Personal Firewall 3.12

Type of Firewall	Personal
OS	Self-Contained
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Armor2net
Availability	*http://www.armor2net.com*

BullGuard® Internet Security 8.5

Abstract

BullGuard® Internet Security is built exclusively for the everyday user. Email, shop, bank, and back up photos and music online and protect your computer from online threats like identity theft, credit card fraud, hackers, spam, viruses, and spyware.

Key features

- **Antivirus**
- **Antispyware**—Protect yourself from identity theft and online fraud.
- **Virus scan and removal**—Search out and destroy viruses that might already be on your computer.
- **Firewall**—Protect your computer from unwanted intruders like hackers.
- **Spamfilter**—Keep your inbox clean from junk mail and phishing attempts.
- **Back-up**—Secure your important files from computer crashes, damage, and theft.
- **Support**—Free 24/7 live support in plain English.

BullGuard 8.5

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	BullGuard
Availability	*http://www.bullguard.com*

CA® Internet Security Suite Plus 2009

Abstract

CA® Internet Security Suite Plus 2009 provides protection against Internet threats that can jeopardize privacy and diminish PC performance. It helps keep important files, photos, music, and settings safe and lets you back them up, restore them, or transfer them to a new PC.

Includes

- Antivirus
- Anti-spyware
- Personal firewall
- Anti-spam
- Anti-phishing
- Parental controls

CA Internet Security Suite Plus 2009

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	eTrust
Availability	*http://shop.ca.com/malware/internet_security_suite.aspx?ggus=36839790&gclid=CNSgibP-85oCFQNaFQodZjHCeQ*

Comodo Personal Firewall

Abstract

Comodo Firewall constantly monitors and defends your PC from Internet attacks.

Features

- Keeps you updated on suspicious files.
- Prevention-based technology stops viruses.
- Default deny protection so only safe files execute.
- Easily learns your PC habits for personalized alerts.
- Automatic updates for the most current protection.

Comodo Personal Firewall

Type of Firewall	Personal
OS	Windows
Hardware	
License	Shareware
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Comodo
Availability	*http://personalfirewall.comodo.com/*

Fireball CyberProtection Suite

Abstract

The Fireball CyberProtection program combines a personal firewall, intrusion detection system, privacy controls, system assessment, parental controls, and an IPsec VPN in a single integrated software suite.

Fireball CyberProtection Suite

Type of Firewall	Personal
OS	Windows
Hardware	
License	Shareware
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	RedCannon
Availability	*http://www.tucows.com/preview/325319*

Freedom Firewall

Abstract

Freedom Firewall provides protection against malicious hackers and security threats while on the Internet. Freedom Firewall software automatically blocks intrusions and hostile attacks. Freedom Firewall not only acts as a shield for your system, but it also boasts additional security features to make your Internet experience more secure.

Features

- Intrusion detection
- Real time alerts to inform you of who's trying to connect to your PC
- Program scan warns you if your programs are trying to send information without your consent
- Detailed intrusion logs to see all blocked intrusions
- Customizable features for advanced users' requirements
- Free updates so you always have the latest version without hassles

This tool has not been updated since Version 4.2, possibly indicating a lack of updates or a discontinuation of the tool.

Freedom Firewall

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Freedom
Availability	*http://personal-firewall-software-review.toptenreviews.com/freedom-firewall-review.html*

F-Secure® Internet Security 2009

Abstract

F-Secure® Internet Security™ protects your data and privacy when you send email, download music, bank, shop, or play online.

Internet Security provides protection against online threats with detection and removal of malicious software. Automatic updates and advanced DeepGuard™ 2.0 cloud computing technology ensure protection against new threats. This security package also includes a firewall, spam control, rootkit detection, and parental control.

Features

- Protects your computer against viruses, worms, and rootkits
- Includes real-time protection against spyware
- Protects your computer against hackers
- Helps you stay free from spam email
- Provides application control
- Easy to install and use
- Protection against new virus outbreaks
- Security news

F Secure Internet Security 2009

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	F-Secure
Availability	*http://www.f-secure.com/en_EMEA/products/home-office/internet-security/index.html*

Personal

Kaspersky® Internet Security 2010

Abstract

Kaspersky® Internet Security 2010, developed by Kaspersky Labs is configurable and has five security levels for ease of use. It is fully compatible with Windows XP and Vista (32/64 bit).

Features

- **Kaspersky Urgent Detection System**—Offers real-time protection while surfing the Web, use Web mail or downloading files.
- **Kaspersky Security Analyzer**—Scans applications to verify application versions and patches.
- **Kaspersky Safe Run**—Runs applications and browsers in an isolated location, preventing access to private data or computer resources.
- **Auto-Run Disable**—Prevent peripherals like portable USB drives from automatically executing when they are plugged in to the machine, prompting users to scan the drive for any hidden threats.
- **Kaspersky iSwift and iChecker Scanning**—Automatically adjusts scanning as your activity increases. Efficiently scans only files that have changed since your last scan.
- **Automated Hourly Updating**—Kaspersky delivers especially small signature updates.
- **Kaspersky Virtual Keyboard**—On-screen keyboard avoids malicious keylogger software
- **Kaspersky Security Network**—Immediate global threat intelligence gathered by the Kaspersky Security Network, which links millions of participating Kaspersky users from around the globe.
- **Kaspersky Whitelisting and Application Control**—Delivers threat intelligence to determine security privileges for every activated application.
- **Kaspersky Anti-Spam and Two-Way Firewall**
- **Kaspersky URL Advisor**—Plug-in for Internet Explorer and Firefox to warn of potentially malicious links.
- **Parental Controls**—Protects children online by limiting time and access to inappropriate sites, instant messaging, games, and online auctions.

Kaspersky Internet Security 2010

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Kaspersky
Availability	*http://www.kaspersky.com/kaspersky_internet_security*

Mac® OS X Firewall

Abstract

Secure Default Configuration
Apple's approach to security protects your Mac® from attacks over private or public networks such as the Internet. All the communication ports are closed and all native services—personal file sharing, Windows file sharing, personal Web sharing, remote login, FTP access, remote Apple events and printer sharing—are turned off by default. The Mac OS X administrator account disables access to the core functions of the operating system.

A new application-based firewall makes it easier for non-experts to get the benefits of firewall protection. The new firewall allows or blocks incoming connections on a per-application basis rather than on a per-port basis.

Users can restrict firewall access to just essential network services (such as those needed for DHCP, bootstrap protocol, IPsec VPNs, and Bonjour), or they can allow (or block) access to selected applications on an individual basis. The application firewall uses digital signatures to verify the identity of applications. If you select an unsigned application, Leopard will sign that application in order to uniquely identify it. For expert users, the IPFW firewall is still available on the system. Because IPFW handles packets at a lower level of the networking stack than the application firewall, its rules take precedence.

Mac OS X Firewall

Type of Firewall	Personal
OS	Mac OS
Hardware	
License	Freeware
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Apple
Availability	*http://www.apple.com/sg/macosx/features/security/*

Norman Personal Firewall

Abstract

This security program utilizes computer and port stealthing technology to ensure your computer is invisible to hackers. The advanced stateful inspection of incoming and outgoing traffic controls data sessions and prevents your computer from being used in botnets, hijacked, or exposed by other hostile activities.

Features

- Hacker protection
- Stateful inspection
- Advanced log utility
- Two-way traffic control
- Works with other security software
- Setup wizard based on user experience

Product benefits

- Real-time protection against hackers and malicious Web robots by filtering inbound and outbound traffic as well as alerting you of attempted attacks
- Two-way firewall filters both incoming and outgoing data traffic blocking external machines trying to connect to the computer, as well as applications on the computer that are trying to connect to other systems on the network
- Launcher protection that detects attempts from an application to launch itself through another application
- Stealth launch protection that uncovers malicious applications attempting to access the Internet *via* other applications. The Personal Firewall keeps track of all parent applications.
- Process hijacking protection detects and reports trojans and spyware attempting to hijack legitimate applications by inserting malicious code.
- Full-stealth mode that ensures that all ports on your computer are completely invisible from the outside

Norman Personal Firewall

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Norman
Availability	*http://www.norman.com/home/all_products/personal_firewall/norman_personal_firewall/en-us*

Norton® Personal Firewall

Abstract

Norton® Internet Security 2009 provides antivirus, spyware and internet protection while you're on the Internet.

Features

- Antivirus
- Spyware protection
- Two-way firewall
- Identity protection
- Antiphishing
- Network security
- Malicious code protection
- Botnet protection
- Rootkit detection
- Browser protection
- Intrusion prevention
- OS and application protection
- Web site authentication
- Pulse updates
- Norton Insight
- SONAR behavioral protection
- Antispam
- Parental controls & confidential information blocking
- Recovery tool
- Norton Protection System

Norton Personal Firewall

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Symantec
Availability	*http://www.symantec.com/norton/products/internet-security.jsp*

Norton Internet Security for Mac

Abstract

The Norton Internet Security suite for Macintosh® is an integrated, nonintrusive security suite with a simple, easy-to-use interface that includes protection found in Norton AntiVirus™ 11 for Mac®, Norton™ Confidential, and two-way firewall functionality. The tool automatically detects and removes spyware, viruses, Trojan horses, malware, and Internet worms.

Features

- Antivirus
- Anti-phishing
- Identity protection
- Internet worm protection
- Two-way firewall
- Vulnerability protection
- Intrusion protection
- Norton DeepSight™
- Browser protection
- File protection

Norton Internet Security for Mac

Type of Firewall	Personal
OS	Mac OSX
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Symantec
Availability	*http://www.symantec.com/norton/macintosh/internet-security*

Outpost Firewall Pro® Version 6.5.4

Abstract

Outpost Firewall Pro® stops malware and hacker attacks before they can activate, by monitoring and controlling Internet access at all times. It does most of its work automatically, so users are not interrupted while they are working. Outpost Firewall Pro is protection that is lightweight, customizable, reliable, and easy to use.

Outpost Firewall PRO Benefits

- Two-way firewall to guard network access
- IDS and ethernet protection for automated defense against vulnerability probes and international breaches
- Anti-spyware to fend off basic malware attacks
- Host protection for proactively blocking unknown threats
- Web and transaction security to protect against Web-borne risks
- Self-protection to maintain continuity of protection
- Automated, updatable configurations to simplify work

Outpost Firewall Pro

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Agtnitum
Availability	*http://www.agnitum.com/products/outpost/*

Trend Micro® Internet Security 2008

Abstract

Trend Micro® Internet Security 2008 provides protection against viruses, Trojan horse programs, worms, and other threats, including network viruses and root kits. It also blocks spyware, hackers, phishing fraud attempts, and unwanted Web sites. It can filter email messages for spam as well.

Features

- Antivirus security
- Spyware protection
- Phishing fraud defense
- WiFi ID
- Spam filtering
- Personal firewall

Trend Micro® Internet Security 2008

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Trend Micro
Availability	*http://us.trendmicro.com/us/products/personal/internet-security/index.html*

Preventon® Personal Firewall Pro

Abstract

Preventon® Personal Firewall Pro offers users protection from hacking attacks. As part of the Preventon Secure Internet Desktop (PSID) series of suites, Preventon Personal Firewall Pro's subscription-based platform enables ISP customers to protect themselves from hacking, Trojan, and automated attack threats.

Preventon Personal Firewall Pro presents a small 'digital footprint' that is suitable for quick download over dial-up and also dispenses with the requirement for regular patches and library updates to be downloaded.

Preventon Personal Firewall Pro offers to ISPs for their customers, a monthly subscription to the software—

- **Firewall protection**—Statistics show the ISP is one of the first points of call for users if they suspect that hackers have infiltrated their PCs.
- Customers may elect to deploy Preventon's products under their own corporate brand.
- **Low support overhead**—A simple-to-use, "apPropriate" interface is used in all Preventon products, which are aimed at the non technical user, who is never presented with jargon or complex dialogues.
- **Low cost deployment of a true subscription system**—Minimal upfront investment required to begin roll out of any of Preventon's products.

Prevention Personal Firewall Pro

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Preventon
Availability	*http://www.preventon.com/firewall.php*

PrivacyWare Privatefirewall 6.0

Abstract

Privatefirewall 6.0 is a Personal Firewall and Intrusion Prevention Application that eliminates unauthorized access to your PC and protects your computer and personal information from hackers, spyware, and viurses. Privatefirewall is easy to install/use. Privatefirewall's interfaces allow advanced users to easily adjust default settings to create custom configurations. Features include: packet filtering, port scanning, IP/Web site protection, email and system anomaly detection, process detection and monitoring, and advanced application protection.

PrivacyWare Privatefirewall 6.0

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	PrivacyWare
Availability	

SurfSecret® Personal Firewall

Abstract

SurfSecret® Personal Firewall is a limited firewall based on surfing security. Its features are associated with a small number of programs. The select options on the management panel provide some room for customization with few advanced features. Port blocking is not available, but it does have options for the major Web browser flavors.

Features

- Three security levels—Maximum, Stealth, and Low
- Emergency lockdown switch
- Customizable lockdown scenarios on screensaver or at time of day
- Filter Installation Wizard specifies exactly which IP addresses are permitted to connect to which ports on your computer
- IP address range and IP address mask support
- At your request, SurfSecret Personal Firewall will display a message every time a packet is blocked
- Detailed logging of break in attempts to application and/or file
- Blocked packet counter
- Automatically checks for new updates and prompts with upgrade instructions
- SurfSecret™ Personal Firewall will run constantly in the background without any user intervention.
- SurfSecret™ Personal Firewall runs on Windows 95, 98, NT, ME, 2000, and XP

SurfSecret Personal Firewall

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	SurfSecret
Availability	*http://personal-firewall-software-review.toptenreviews.com/surfsecret-personal-firewall-software.html*

The DoorStop X Firewall

Abstract

DoorStop X Firewall 2.2 is available for Mac OS X 10.5 or later. You may download a free, fully functional, 30-day evaluation version. You may purchase DoorStop either individually or as part of the integrated DoorStop X Security Suite.

Features

- Easy-to-use main window with built-in standard Mac OS X services
- All TCP services protected by default
- Ability to tune protection on a service by service and address by address basis
- Protect services by name or port number
- Default protection setting that applies to all unspecified services
- Four protection modes: deny all, permit all, permit by address, deny by address
- Full logging of permitted and/or denied connections. Integrated with our "Who's There?" Firewall Advisor to help you understand, analyze, and react to access attempts
- Includes a built-in version of "Internet Security for Your Macintosh: A Guide for the Rest of Us," browsable on a service-by-service or section-by-section basis
- Status menu item available at all times helps confirm that DoorStop is active
- Optional protection and logging for User Datagram Protocol (UDP) services and ports
- Stealth mode
- Updated with newest service names and ports

The DoorStop X Firewall

Type of Firewall	Personal
OS	Mac OS
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Open Door Networks
Availability	*http://www.opendoor.com/doorstop*

Webroot® Desktop Firewall

Abstract

Webroot® Desktop Firewall secures your computer from Internet threats and reduces the risks of being a victim of online crimes. Designed for novices and experts, Webroot Desktop Firewall performs the following—

- Monitors Internet traffic in and out of your PC for better protection
- "Hides" your PC from online scammers looking for easy targets
- Prevents remote access Trojans from hijacking your PC

Webroot Desktop Firewall actively monitors activity and alerts you to suspicious traffic so you aren't surprised by unwanted traffic.

Webroot Desktop Firewall lets your computer operate in Stealth Mode, making your online presence invisible to Internet scammers looking for easy targets.

Webroot Desktop Firewall

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Webroot
Availability	*http://www.webroot.com/consumer/products/desktopfirewall*

Windows Firewall

Abstract

Windows Firewall, previously known as Internet Connection Firewall (ICF), is a protective boundary that monitors and restricts information that travels between your computer and a network or the Internet. This provides a line of defense against someone who may try to access your computer from outside the Windows Firewall without your permission.

If you are running Windows XP Service Pack 2 (SP2), Windows Firewall is turned on by default; however, some computer manufacturers and network administrators might turn it off.

When someone on the Internet or on a network tries to connect to your computer, we call that attempt an "unsolicited request." When your computer gets an unsolicited request, Windows Firewall blocks the connection. If you run a program, such as an instant messaging (IM) program or a multi-player network game that requires information from the Internet or a network, the firewall asks if you want to block or unblock (permit) the connection.

If you choose to unblock the connection, Windows Firewall creates an exception so that the firewall will not bother you when that program needs to receive that information in the future.

Windows Firewall

Type of Firewall	Personal
OS	Windows
Hardware	
License	Freeware
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Microsoft
Availability	*http://www.microsoft.com/windowsxp/using/security/Internet/sp2_wfintro.mspx*

ZoneAlarm® and ZoneAlarm® Pro

Abstract

ZoneAlarm® and ZoneAlarm® Pro protects a PC from hackers, spyware, and other Internet threats—

- **Network Firewall**—Stateful stealth firewall guards the network perimeter from inbound and outbound threats.
- **Program Firewall**—A second firewall layer surrounds each software program, protecting good programs from bad.
- **OS Firewall**—The third firewall layer goes down to the kernel to protect the operating system, including the registry and file systems, from attack by malicious programs.

Features

- Scans for and removes thousands of spyware traces from your computer
- Provides your PC with real-time security updates and new attack protection capabilities
- Protects you from identity theft and online profiling
- Quarantines suspicious attachments to help defend against unknown viruses
- Automatically halts outbound messages to keep you from accidentally infecting others
- Automatically detects wireless networks and secures your PC from hackers and other Internet threats wherever you are connected

ZoneAlarm and ZoneAlarm Pro

Type of Firewall	Personal
OS	Windows
Hardware	
License	Commercial
National Information Assurance Partnership (NIAP) Validated	False
Common Criteria	
Developer	Check Point
Availability	*http://www.zonealarm.com/security/en-us/computer-security.htm*

SECTION 7 ▶ Definitions of Acronyms and Key Terms

Acronym or Term	Definition
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
API	Application Programming Interface
Application-Level Gateway	The application-level gateway acts as a proxy for applications, performing all data exchanges with the remote system on their behalf.
APS	Application Protection System
ARP	Address Resolution Protocol
ASIC	Application Specific Integrated Circuit
BGP	Border Gateway Protocol
BSD	Berkeley Software Distribution
CCEVS	Common Criteria Evaluation and Validation Scheme
Circuit-Level Gateway	Circuit-level gateways work at the session layer of the OSI model or between the application layer and the transport layer of the TCP/IP stack. They monitor TCP handshaking between packets to determine whether a requested session is legitimate.
CoS	Class of Service
DHCP	Dynamic Host Configuration Protocol—A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.
DiD	Defense in Depth
DMZ	Demilitarized Zone
DNS	Domain Name Server
DoD	Department of Defense
DoS	Denial of Service
DSCP	Differentiated Services Code Points
DTIC	Defense Technical Information Center
EAL	Evaluation Assurance Level (Common Criteria)
Firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets. All messages entering or leaving the Intranet pass through the firewall, which examines each message and blocks those that do not meet specified security criteria.
FTP	File Transfer Protocol
FWPD	Firewall Product Developer
GET	An HTTP command used to request information from a Web server
GTA	Global Technology Associates (Inc.)
GUI	Graphical User Interface

Acronym or Term	Definition
Hacker	A person who either breaks into systems for which he or she has no authorization or intentionally oversteps bounds on systems for which the hacker has legitimate access (*i.e.,* an unauthorized individual who attempts to penetrate information systems to browse, steal, or modify data; deny access or service to others; or cause damage or harm in some other way)
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IAC	Information Analysis Center
IATAC	Information Assurance Technology Analysis Center
ICF	Internet Connection Firewall
ICMP	Internet Control Message Protocol
ICSA	International Computer Security Association
ID	Intrusion Detection
IDS	Intrusion Detection System—Inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system
IM	Instant Messaging
IOS	Internetworking Operating System
IP	Internet Protocol—A standardized method of transporting information across the Internet in packets of data. It is often linked to Transmission Control Protocol (TCP), which assembles the packets once they have been delivered to the intended location.
IPFW	Internet Protocol Firewall
IPS	Intrusion Prevention System
IPsec	Secure Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISA	Internet Security and Acceleration
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
Malicious Code	Malicious code includes any and all programs (including macros and scripts) that are deliberately coded to cause an unexpected (and usually unwanted) event on a PC or other system.
NAPT	Network Address Port Translation
NAT	Network Address Translation—An Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic
Network	A group of computers linked together to share information. Networks can consist of a number of linked computers in a specific physical location—a Local Area Network (LAN)—or they may consist of computers located at different physical sites linked together by means of phone lines and modems or other forms of long distance communications.
NIAP	National Information Assurance Partnership

Acronym or Term	Definition
NIC	Network Interface Card—An expansion board inserted into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.
NIPS	Network Intrusion Prevention System
NSA	Network Security Appliance
OOTP	Object Oriented Transparent Proxying
OS	Operating System
OSI	Open System Interconnection
OSPF	Open Shortest Path First
Packet	A unit of data sent across a network. When a large block of data is to be sent over a network, it is broken up into several packets, sent, and then reassembled at its destination. Packets often include checksum codes to detect transmission errors. The exact layout of an individual packet is determined by the protocol being used.
Packet Filter	Rules used by a firewall to accept or reject incoming network communication packets based on source and destination IP addresses, source and destination port numbers, and packet type. These rules can also be used to reject any packet from the outside that claims to come from an address inside the network.
PAD	Protocol Anomaly Detection
PAT	Port Address Translation
PBX	Private Branch Exchange
PCRE	Perl Compatible Regular Expressions
PIX	Private Internet Exchange (Cisco)
POP3	Post Office Protocol version 3
Proxy	A software agent that performs a function or operation on behalf of another application or system while hiding the details involved
PSID	PreventonTM Secure Internet Desktop
QoS	Quality of Service
QUADRO	Queues and Delays at Roadworks
RIP	Routing Information Protocol
Router	A device that determines the next network point to which a data packet should be forwarded en route to its destination. The router is connected to at least two networks and determines which way to send each data packet based on its current understanding of the state of the networks to which it is connected. Routers create or maintain a table of available routes and use this information to determine the best route for a given data packet.
RPC	Remote Procedure Call
RTSP	Real Time Streaming Protocol
SEM	Security Event Management
SIP	Session Initiation Protocol
SMB	Small and Medium-Sized Business
SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SPI	Stateful Packet Inspection

Acronym or Term	Definition
SSA	Stateful Signature Analysis
SSL	Secure Socket Layer
Stateful Multilevel Inspection	Filters packets at the network layer, determines whether session packets are legitimate, and evaluates contents of packets at the application layer
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol—The Internet standard transport protocol that provides the reliable, two-way connected service that allows an application to send a stream of data end-to-end between two computers across a network
TDM	Telephone Directory Monitor
TLS	Transport Layer Security
UDP	User Datagram Protocol—A connectionless protocol that, as does TCP, runs atop IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network
UPnP	Universal Plug and Play
URL	Universal Resource Locator
UTD	Unified Threat Defense
UTM	Unified Threat Management
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network—A private network built atop a public network. Hosts within the private network use encryption to talk to other hosts; the encryption excludes hosts from outside the private network, even though they are on the public network.
Vulnerability	Hardware, firmware, or software flow that leaves a system open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, *etc.*, that could be exploited by a threat to gain unauthorized access to information or to disrupt critical processing.
WAN	Wide Area Network
WiFi	Wireless Fidelity